 DOI: https://doi.org/10.26549/bdai.v4i2.13133

Research on the Application of Data Encryption Technology in Computer Network Security

Song Yue Rui Cao Zhengqi Zhang Bo Lu

Xinjiang Information Industry Co., Ltd., Urumqi, Xinjiang, 830000, China

Abstract

In recent years, the attention of the computer network security has been improved, the new technology also plays a practical value in the computer network security, the effect is obvious. Data encryption technology is the product of the new era, which is of great significance to guarantee the security of computer network. This paper will summarize its specific application situation, and put forward reasonable suggestions for practical ideas, aiming to give full play to a certain reference value.

Keywords

data encryption technology; computer network security; application practice

数据加密技术在计算机网络安全中的应用研究

岳松 曹蕊 张郑齐 鲁博

新疆信息产业有限责任公司，中国·新疆 乌鲁木齐 830000

摘 要

近年来，计算机网络安全受到的关注度有所提升，新型技术也在计算机网络安全中发挥出实际价值，效果明显。数据加密技术是新时代的产物，对于保障计算机网络安全意义重大，论文将概述其具体应用情况，针对实践思路提出合理建议，旨在发挥出一定的参考价值。

关键词

数据加密技术；计算机网络安全；应用实践

1 引言

目前，大数据技术应用范围持续扩大，计算机网络安全问题却成为了热议话题，对于人们的生产生活能够产生直接影响。在计算机网络运行的过程中，数据加密技术能够发挥出自身价值，通过提升计算机网络安全性和可靠性，可以控制信息资源的泄露概率，保障资源传播环节的稳定。

2 数据加密技术概述

数据加密技术重点是指让信息通过加密钥和加密函数转换，由此呈现出无意义的密文，接收方则是让此密文在解密钥和解密函数的支持下还原成明文。在使用数据加密技术时，应该明确其重点涵盖的内容，要明确技术支撑条件。

2.1 专用密钥

所谓的专用密钥，就是指的对称密钥和单密钥，通过使用同一个密钥，也就是同一个算法，使得相应的信息得以保护，发挥出实际的利用作用。在文本加密传输的过程中，会运用到密钥加密成密文，这样便可安全地在信道上传输，当收到相应的密文后，经过针对性解密，就能形成普通文体以供使用[1]。

2.2 对称密钥

对称密钥属于相对古老的手段，如密电码就是采用了对称密钥，因为运量小且速度较快，所以现阶段仍然受到广泛关注。如 DES 就是一种数据分组的加密算法，主要是将数据分成长度是 64 位的数据块，其中 8 位用作奇偶校验，剩余的 56 位作为密码的长度。通过原文的置换，获取 64 位杂乱无章的数据组，然后细化出两段，再通过加密函数变换，结合给定的密钥参数分析，在多次迭代中获取加密密文。

2.3 公开密钥

公开密钥也属于非对称密钥，加密与解密的过程中需要运用不同的密钥，也就是不同算法，尽管二者间的关系密切，但是不会轻易推算出另外一个。

非对称密钥中的加密密钥和解密密钥存在明显差异，所以可以将一个密钥公开，另外一个则是保密，由此便会发挥出理想的加密效果。

编码环节，一个密码主要是加密消息，另外一个则是

【作者简介】岳松（1986–），男，中国新疆五家渠人，本科，助理工程师，从事网络安全研究。

发挥出解密作用。

公开密钥的加密机制具有理想的保密效果，但是无法辨明信息发送者，也就是任何获取公开密钥的人都能生成并发送报文。

2.4 非对称加密技术

数字签名多是运用了非对称加密技术，重点是对整个明文进行变换，由此获取数值，当做核实签名。接收者使用发送者的公开密钥对签名解密运算，若是结果为明文，则证实了对方身份真实可靠。签名也可以运用多重措施，比如将签名附于明文后，数字签名基本是运用至电子贸易和银行等领域。

数据加密技术信息传输见图 1。

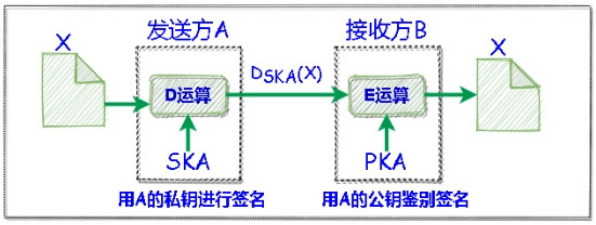

图 1 数据加密技术信息传输示意图

3 计算机网络安全现状

3.1 多元化黑客入侵方式

黑客是影响计算机网络安全的重要因素之一，其会让计算机网络数据出现大面积丢失的情况，最终影响到正常的使用。黑客一般是在网络系统中出现，随着相关技术的飞速发展，黑客的侵入方式也更加多元。若是未能控制这类非法入侵的行为，将会引发更为严重的后果，使计算机网络系统逐渐瘫痪，其中的重要信息也会被随意窃取，最终给企业和个人造成巨大损失。

3.2 计算机病毒干扰较大

计算机病毒是影响网络运行的关键，属于干扰计算机网络体系安全运行的核心因素 [2]。计算机病毒主要是在先进技术的支撑下寻找切入点，进而在计算机网络系统中植入病毒，非法获取其中的信息资源。因为计算机技术的发展速度较快，计算机病毒的种类也是日渐增多，破坏力明显增强。

3.3 人为影响严重

计算机网络一般是依靠着人为操作加以运行，以此才能呈现出所需要的信息，保证质量成果达到最佳。但是因为人为主观意识较强，所以在具体操作中极易干扰网络运行的情况，若是相关人员的素质水平偏低，加之忽视了对密码的有效保护，将会直接引发网络安全问题，给病毒侵入创造机会，威胁到企业或者是个人的信息安全。

数据加密技术流程见图 2。

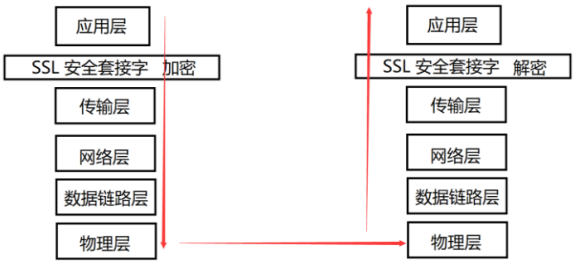

图 2 数据加密技术流程图

4 数据加密技术在计算机网络安全中的应用要点

4.1 准确评估安全等级

新的时代背景下，计算机网络安全受到的关注度明显提升，其关系到各方主体的切身利益，应该重视数据加密技术的应用方向，让其在计算机网络运行中发挥出可靠的保护效果。计算机加密技术应用环节，应该重视其实际特点，还要重视安全等级的准确评估，分析应用的可靠性。数据加密技术应用效果备受认可，因此展示出强大的防御性能，具体的安全性和稳定性也能反映出来。在对计算机网络进行有效性分析时，必须采取合理措施规范数据加密技术的应用，这样才能对整个网络系统的安全提供保障，使其拥有相对稳固的条件。

4.2 强化系统防御能力

数据加密技术并不是单纯地停留在算法层面，还是依靠着网络体系生成的针对性措施，这也证实了数据加密技术的应用价值，可以稳步提升数据信息的精准性和可靠性。数据在传输的环节保持稳定状态，经过资源的有效叠合，让计算机网络传输过程更加可靠，规避错误网络数据 [3]。目前，网络安全技术的全面支持下，数据加密技术应用范围逐步拓宽，为了更好的满足多重需求，数据加密技术也不是采用单一的加密方式，而是让多种加密方式组合起来，促使着数据信息更加安全。

5 数据加密技术在计算机网络安全中的应用思路

5.1 节点加密技术

数据加密技术的应用中，基本目标是让计算机网络系统运行获取支撑条件，由此维护系统的稳定运行。整个过程中，数据加密技术发挥出理想效果，可以防范数据信息在上传以及下载过程中随意丢失，以免被恶意攻击和改写。在数据加密技术全面发展的背景下，多种技术类型日渐丰富起来，这对保护网络的安全及可靠意义重大。现阶段，选择相关的数据加密技术时，节点加密技术受到广泛关注，其被运用至计算机网络中，能够提升数据信息的安全性，防范资源丢失，让数据传播更加安全。

5.2 链路加密技术

相较于节点加密技术，链路加密技术的应用效果更尽人意，核心优势在于各个节点链路都能进行针对性加密，强化网络系统中数据加密的效果[4]。在运用相关的技术措施时，了解到相关的应用范围较大，结合维度分析，链路加密技术除了可以实现对各个节点的针对性加密外，还能完成对多种网络信息的同步加密，保证实际的加密效果达到最佳。基于此，链路加密技术充分展示出数据加密技术的优势，也让多种网络信息聚集到一起，更好地完成同步处理，保证了全过程的安全和可靠。除了这样的操作细节，在采取相关的技术措施时，还能实现二次加密处理目标，让多种信息资源保护效果进一步优化。

5.3 端到端的加密技术

端到端的加密技术应用时间较短，但是也能发挥出实际的效果，可以让计算机网络数据加密效果充分显现出来。在具体应用的过程中，这种技术的优势更加突出，相较于节点加密技术和链路加密技术，其能实现数据传输流程的加密，促使着整个过程更加安全，防范传输环节埋下安全隐患，安全性更高。

6 数据加密技术在计算机网络安全中的应用实践

6.1 计算机软件中的应用实践

计算机网络系统运行阶段，重点是将硬件当作重要条件，硬件若是无法支撑计算机系统的运行，将会失去存在价值，难以保证信息安全。硬件也是决定计算机系统各项性能的关键因素，对于安全具有保障作用，要关注数据加密技术的实际应用情况。

6.1.1 保护用户信息

在数据加密技术的应用中，计算机网络能够获取可靠的保障条件，让用户在使用网络时及时地防范多重隐患。通过输入正确密码，获取对应的权限，在规定时间段内完成数据浏览和复制等一系列动作，避免出现各种各样的问题。

6.1.2 辨明风险因素

如果计算机软件系统受到外界因素的干扰，数据加密系统可以展示出强大功能，通过快速地辨明风险因素，明确其具体位置，在短时间内采取可靠的防御措施[5]。另外，适当地运用杀毒软件，可以将系统内部病毒妥善清理，让计算机系统趋向稳定，保持相对安全的状态。

6.2 电子商务中的应用实践

互联网技术飞速发展的背景下，电子商务技术应运而生，其对各个企业的发展做出了巨大贡献。在新型手段的支撑之下，电子商务发挥出自身优势，其将多个主体有效串联，打造出完整供应链，带动产业进步和发展。在电子商务产业持续前进的背景下，数据安全问题显现出来，通过融入数据加密技术，让电子商务产业发展更加稳定，拥有相对理想的支撑条件。

6.3 局域网中的应用实践

技术发展与革新的目标就是让用户们获取绝佳体验，通过提供优质服务，使得信息安全得以保障，提升整体的应用实效。现阶段，数据加密技术成功融入大众视野，各个行业也开始重视到此项技术的优势，相关人员要结合应用方向加以分析，结合数据加密技术的特征优化举措，确保信息资源的漏洞及隐患及时查明，采取合理的应对措施。在局域网中，相关技术也能发挥出自身价值，如企业开展食品会议和数据汇总等工作时，可以借助具体手段强化信息资源安全性和可靠性，保证整体的效益成果。

7 结语

综上所述，数据加密技术就是新时代的产物，对于计算机网络安全影响较大，应该肯定其优势，让其为相关实践提供参考。数据加密技术的应用阶段，除了提升计算机网络安全性和稳定性外，也可避免错误数据，使工作人员获取参考依据，给各项工作的开展稳固基础。

参考文献

[1] 王丽华.数据加密技术在计算机网络安全实践中的应用——评《计算机网络技术及应用》[J].中国科技论文,2023,18(2):245.

[2] 叶青,郑路攀,祝勇,等.基于分布式区块链与信息加密技术的电力工程数据共享策略设计[J].电子设计工程,2023,31(2):121-125.

[3] 李容嵩,彭凌烟,蒋成,张定军.基于区块链和属性加密的工程检测数据安全共享技术研究[J].湖南电力,2022,42(3):65-72.

[4] 时春波,李卫东,秦丹阳,等.Python环境下利用Selenium与JavaScript逆向技术爬虫研究[J].河南科技,2022,41(10):20-23.

[5] 冯聪.运用大数据资源与区块链技术办理涉数字货币犯罪的实践与构想[J].信息网络安全,2021(S1):50-53.