数据加密技术在计算机网络安全中的实践探讨

葛 庆

（数字广西集团有限公司，广西 南宁 545000）

摘 要 计算机信息技术已经渗透到人们日常生活及工作的方方面面，实现了对我国社会现代化发展的有效促进，但在当前网络环境下，计算机网络安全问题依然较为严峻，主要由于计算机网络开放性特征越来越明显，使得信息传递交流过程中出现信息丢失、信息被盗的可能性明显加大，这就需要有相应的加密技术对其进行支持。数据加密技术已经在当前计算机网络安全中有广泛应用，通过数据加密技术的算法、密钥的合理使用，可以使计算机信息技术优势得到充分体现，能够对多种格式的计算机文件进行加密处理，进而保证计算机信息系统数据安全性，降低非法分子入侵的可能性。因此，本文从计算机网络系统数据加密技术原理及类型分析入手，并对当前计算机网络面临的操作系统、数据管理系统、网络环境等潜在安全隐患及具体问题进行了分析，对数据加密技术在计算机网络安全中的实践应用进行了探讨，希望能为保障今后我国计算机网络系统安全运行提供参考。

关键词 数据加密技术；计算机网络安全；密钥管理

中图分类号：TP393.08 **文献标识码**：A **文章编号**：2097-3365(2023)12-0010-03

由于当前计算机网络信息技术已经在我国高度普及，因此，加大计算机网络安全管控至关重要，其可以保证计算机信息技术在给人们带来便利的同时，数据信息被非法盗取、破坏的可能性明显降低，进而使文件信息的传输与保存更为安全便捷。由此可以看出，在保证计算机网络信息技术使用便捷性的同时，必须将提高计算机网络信息数据传递及储存安全性作为重要工作，这样才能使计算机信息技术的实际应用成效得到充分体现。数据加密技术已经成为当前计算机网络安全中的重要组成部分，如果不能保证数据加密技术选用的科学性及针对性，则会使网络通信安全受到严重威胁，因此，对数据加密技术在计算机网络安全中的实践应用进行深入分析非常有必要。

1 我国计算机网络安全现状分析

就我国当前计算机网络信息技术使用情况来看，网络安全问题依然不容小觑，虽然我国已经出台了与之相应的法规制度，但从整体来看，对网络环境及数据信息传输安全的管控效果依然有待优化。而对于数据加密技术而言，其已经成为保障我国计算机网络安全的重要技术体系，在计算机网络环境中的应用越来越广泛，成为计算机网络系统稳定运转必不可少的关键技术[1]。

2 数据加密技术原理及类型分析

数据加密技术是一种重要的信息安全保障技术体系，在实际执行过程中，数据加密技术主要是通过特定的算法来将明文转化为密文，进而达到对数据信息安全的有效保证，使得未经授权的人无法读取密文，更加无法对密文进行人为修改，这也使得数据信息的完整性、安全性得到了保证，同时也使得计算机网络系统之间的信息传输更为流畅、便捷，明显降低了黑客攻击及信息泄露等问题出现的可能性。通过对目前数据加密技术分类，可以将其大致分为对称密钥加密技术、非对称密钥加密技术两种。首先，对称密钥加密技术。对于此种数据加密技术而言，其是当前我国应用最为广泛的计算机网络安全数据加密技术，在对此项技术进行应用时，其主要是通过加密与解密相结合的方式来保证数据信息的安全性，可以看出，其加密速度较快，通常而言，此种数据加密技术适合应用于数据量较小的加密需求，这样可以使对称密钥加密算法的针对性及准确性得到体现[2]。目前最为常见的对称密钥加密算法主要包括DES算法、3DES算法等几种，通过对上述算法的应用，可以使加密效果得到保证，尤其对于DES加密算法而言，其是最早出现的对称密钥加密算法，此种算法的主要优势体现为安全性高，但由于此种密钥算法长度只有56位，因此在落实应用的过程中，受到外界暴力破解及黑客暴力攻击的可能性较大，也正是因为如此，3DES算法应运而生。对于3DES算法而言，其在原有的56位密钥基础上增加了两个56位密钥，从而使得数据加密效果更为理想，明显提高了数据安全性，同时，这种加密算法所适应的场

景更为广泛；其次，非对称密钥加密技术。此项技术也是当前我国计算机网络信息数据加密过程中经常应用的加密技术之一，其主要特点体现为加密与解密所使用的密钥不同，这也使得整个加密过程更为复杂，但与此同时，其安全程度也明显提高[3]。一般来说，在应用非对称密钥加密技术时，需要根据实际需求设定两个密钥，即，一个公钥一个私钥，顾名思义，公钥属于可以公开的密钥，而私钥只有密钥持有者才能解开，这也使得其可以应用于多种场合，同时也保证了整个加密系统的安全性与稳定性。但对于非对称密钥加密技术而言，其在实际应用过程中也体现出了一定的缺陷，主要体现为应用此种数据加密技术的系统往往加密速度较慢，但从整体来看，非对称密钥加密技术依然属于一种较为实用的加密技术，尤其适合应用到数据量较大的加密需求中。

3 当前计算机网络面临的具体安全问题

3.1 操作系统存在安全隐患

从当前计算机网络系统运行情况来看，其所面临的安全问题多种多样，其中，操作系统的安全隐患则是重要体现，之所以操作系统存在安全隐患，往往与计算机病毒入侵有直接关系，当病毒入侵之后，会对计算机系统的正常运行产生影响。而计算机病毒的产生并非偶然，通常是因为黑客编写了对计算机网络系统有破坏作用的程序，并且，这段程序会隐藏在计算机系统的其他可执行程序中，由于其自身具备极强的隐藏及伪装能力，这也使得计算机病毒具有隐蔽性，往往很难被及时发现，再加上其复制及传播迅速，因此会对计算机网络系统安全产生严重威胁[4]。就目前来看，计算机病毒种类较为复杂，无论是互联网病毒、DOS系统病毒等，都可能对计算机数据信息安全产生严重威胁，进而致使计算机网络操作系统存在安全隐患。

3.2 数据管理系统存在安全隐患

对于数据管理系统的安全隐患而言，其主要是指系统漏洞，由于计算机网络系统属于一种人工智能产物，因此在逻辑设定、编译及执行过程中可能会存在某种缺陷，而这一缺陷问题很可能会转化为系统漏洞，正是因为这些系统漏洞客观存在，致使黑客有机会利用这些漏洞植入木马及病毒，一旦植入成功，则会导致计算机网络系统的安全性受到严重威胁，还会导致计算机数据披露及软硬件设备损坏等一系列严重问题发生[5]。通常来讲，计算机网络系统的漏洞，可以通过用户定期运用补丁程序扫描的方式发现，进而对漏洞进行针对性修复，但这种扫描与修复往往很难保证万无一失，并且，经常会出现已有漏洞被发现解决之后，便紧接着出现新的未知漏洞的现象，这也导致系统漏洞具有持续性及随时性，属于计算机网络系统中潜在的危险因素。

3.3 网络环境中存在安全隐患

对于互联网平台而言，其允许用户自由发布各种类型的信息，虽然实现了对信息传递效率及广泛性的有效保证，但往往也面临着较为严峻的网络安全问题，尤其无法保障信息的真实性，并且，用户在网络上自由发布及获取信息的过程中，还可能受到传输线路的攻击或网络协议攻击，也正是因为上述情况存在，导致计算机软件、硬件受攻击的可能性明显加大，进而影响了计算机网络系统的安全性。目前，网络中的协议不安全性因素对计算机网络的影响最为明显，其主要协议包括FTP协议、NFS协议及TCP协议等，如果上述协议存在漏洞，则可能导致入侵者非法入侵，进而实现对用户名的精准检索，并且获得相应密码口令，这样便可以实现对计算机防火墙系统的有效供给，以此达到其非法操控网络信息系统、获取机密信息的目的。

4 数据加密技术在计算机网络安全中的实践应用要点

4.1 保证数据加密技术算法选择针对性

从目前我国计算机网络安全管控工作开展情况来看，所应用的数据加密技术种类众多，想要使数据加密技术的应用成效得到充分体现，应该结合用户自身需求确定具有针对性的加密技术体系，并且要注意对运行环境及运行条件进行合理设定，这样才能使数据加密技术的应用优势得到最大程度的体现。目前，密码技术已经成为我国计算机网络数据加密技术中的重要组成部分，在对密码技术进行应用时，应该根据用户具体需求确定应用对称密钥系统还是非对称密钥系统，如果对加密数据及解密数据的速度有较高要求，应该注意使用对称密钥技术；如果对加密及解密复杂性有较高要求，则要注意使用非对称密钥系统。在上文中提到DES加密算法，其是一种经典的对称密钥算法，同时也是当前数据加密技术中常用的算法之一，在对此种算法进行实际应用时，应该注意先对目标密文进行分组、排列，然后再对其进行针对性处理，最终获得完整的密文，这样才能使加密效果得到保证。而对于MD5加密算法来说，其属于一种较为复杂且精准程度更高的加密方式，在进行数据转变处理时，MD5主要

是以补位、变换的处理方式最终，最终可以输出已经完成加密的密文[6]。并且，MD5 算法具有不可逆的特征，因此，将其应用到计算机网络信息数据加密中时，其加密效果更为理想，数据信息的安全程度也更高。

4.2 优化数据加密技术的系统运行方式及运行环境

想要使数据加密技术在计算机网络安全管控中的实践应用效果得到保证，应该充分意识到系统运行环境对加密效果所产生的具体影响，这就需要在进行计算机硬件及软件选择时，做好相应的系统运行环境匹配及优化。一般来说，计算机设备、服务器等往往存在一定的差异性，也正是因为这种差异性客观存在，使得数据加密及解密的效果存在一定的差别。并且，服务器与服务器之间的数据信息传输方式往往也具有多样化的特征，由于服务器本身负责对所有用户进行过管理，因此，对服务器功能有严格要求，通常需要其具备用户设备的所有功能，这样才能保证数据加密技术体系可以正常运行。对于数据信息的发送方来说，其主要负责将目标文件传输给接收方，并且通过对数据信息进行合理利用的方式来确定针对性更强的、更为具体的上层解密程序，这样才能使整个解密过程更为完整[7]。在整个数据信息传输过程中，要保证系统运行环境的适宜性，这就需要系统根据所传递的数据信息制定出相应的服务器与目标用户，进而保证运行方式及运行环境与之匹配，这也是保证信息传输过程安全性、流畅性的关键。

4.3 强化密钥管理

强化密钥管理是保证数据加密技术应用优势得到最大限度体现的关键路径，尤其要对计算机网络信息明文与密文在不同公式、算法下应遵守的原则进行明确，这样才能使密钥管理成效得到保障。密钥是当前计算机网络信息加密系统中保证解密算法完整性的关键，其重要性不言而喻，因此要注意采用最佳方案来实现密钥管理。一般来说，在计算机系统之间进行正式通信之前，服务端会与客户端完成服务器公钥分发，然后对相应的信息进行保密处理，其中的公钥需要由应用程序自动生成，这样则可以实现对密钥管理的有效强化[8]。在应用 AES 加密算法时，要注意对密钥管理进行深入分析，利用此种算法形成随机密码，这些随机密码往往可以在数据信息被打包之前通过文件打包模块的方式整理好，然后设定相应的用户信息处理权限，拥有最高处理权限的使用者则可以获得所有文件信息[9]。并且，在接收待解密文件时，由于这些文件本身属于系统加密文件，因此，需要服务器自动生成相应的密钥、用户名，并且将其编写到数据库中，这样不仅可以保证信息获取途径合法，同时也使得密码查询及验证的流畅性、高效性得到了保证。

5 结语

总之，由于当前我国计算机网络信息技术水平不断提高，网络信息技术已经走进千家万户，但在享受信息技术便捷性的同时，数据信息安全问题不容小觑，想要保证计算机信息数据安全，则要注意保证计算机网络系统的运行方式及运行环境的适宜性，而数据加密技术的应用则实现了对计算机网络信息数据安全性的有效保证，通过对数据加密技术的合理选择及应用，可以使计算机网络信息技术优势得到充分体现[10]。今后，应该根据计算机网络安全管理实际需求确定数据加密技术的具体应用方向，这样不仅可以为计算机网络系统提供强有力的技术保障，同时也可以使网络环境的稳定性及安全性得到保障，从而促进我国现代化信息技术体系的稳定发展。

参考文献：

[1] 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，2023,10(08):52-55.
[2] 杨鑫．数据加密技术在计算机网络通信安全中的应用分析 [J]. 网络安全技术与应用，2023,24(08):31-32.
[3] 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，2023,11(07):25-27.
[4] 李波，王健光．计算机网络信息安全中数据加密技术的应用研究 [J]. 科技资讯，2023,21(11):10-13.
[5] 宋凯，汪庆伟，张媛媛，等．数据加密技术在计算机网络安全防护中的应用研究 [J]. 中国军转民，2023,23(07):35-36.
[6] 邱玲．大数据技术在计算机网络信息安全处理中的实践分析 [J]. 信息记录材料，2023,24(03):83-85.
[7] 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(02):245.
[8] 张磊，李研，阳生云等．计算机网络信息安全领域中数据加密技术的运用阐述 [J]. 软件，2022,43(11):65-67.
[9] 黄小丽．数据加密技术在计算机网络安全中的应用探究 [C]// 中国管理科学研究院教育科学研究所．教育理论研究与实践网络研讨会论文集（二），2022.
[10] 朱奕捷．简析加密技术在计算机网络信息安全中的地位和作用 [J]. 网络安全技术与应用，2022,14(07):20-21.