数据加密技术在计算机网络安全中的应用探析

郭禹伶[1] 申培培[2]
1. 国网河北省电力有限公司电力科学研究院；2. 国网河北省电力有限公司信息通信分公司

摘要：当前人类社会正处于信息化的时代，因此计算机网络信息的安全应当要受到个人或企业足够的重视，切实保证自身数据信息的安全性。积极采用数据加密技术对计算机网络信息进行加密，保证数据信息不被篡改或窃取，并且还要对数据加密技术不断进行完善，建立有效的防护机制，保障网络信息的安全。基于此，本文主要分析了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；网络信息；安全

一、计算机网络通信安全中数据加密技术应用的重要性

计算机网络通信系统运行中难免会出现各种故障以及漏洞，这也是计算机网络通信安全事故常发的关键原因，如果只是危害性比较小的病毒，防火墙就可以拦截病毒，可是近些年来，随这计算机的数据信息量增多，病毒类型也呈现出多样性，利用防火墙模式进行病毒拦截已经难以满足计算机通信要求，因此，应重视新型数据技术的应用。对计算机网络通信安全处理，目前使用比较广泛的技术就是数据加密技术，数据加密技术可以分为专用密钥、对称密钥、公开密钥、非对称加密技术。其可以保障用户隐私，确保数据更加安全，将计算机网络通信系统中的漏洞弥补，使得计算机可以正常运行，同时也可以促使计算机网络系统通信更加安全。另外，数据加密技术可以将部分特殊数据隐藏，利用密钥可以将网络通信安全数据科学处理，降低重要特殊信息被盗的可能性，可最大限度的防止病毒入侵，达到对于计算机系网络通信信息保密以及保护的作用，增强了计算机网络通信安全效果[1]。

二、数据加密技术在计算机网络安全中的应用

（一）端到端技术

计算机网络中应用端到端技术，其传输形式是密文，主要是指计算机数据信息到本来规定的传输目的地之后，才能对于数据信息进行解密。这种情况，即使数据在中间某一节点传输出现问题，也不会对网络数据信息传输造成影响，其主要适用对象是针对计算机应用层。与其他相关的计算机网络技术相比，其不需要将一些中间环节数据传输解密，其可以将解密设备以及装置数量有效减少，减少网络安全支出的成本，其数据传递稳定性比较高，但是本数据加密技术通常不适用于对于报头数据信息的传递以及加密。若是将其运用于报文加密，网络部分人员可能会通过其对于安全系统攻击，获得传输数据信息，其在数据传递安全性存在不足的问题，并且本数据加密技术也没有办法针对其数据传输的起点以及终点加密。因此，计算机网络人员应了解本数据加密技术的优势以及劣势，并根据具体的用户需求去进行技术的选择，保障其可以得到更加广泛的应用。

（二）链路数据加密技术

链路数据加密技术使用中，计算机会对链路加密，将需要进行传输的计算机网络数据进行处理，在传输未开始前，对其进行加密，之后对于每一个节点所收到数据信息解密，之后就可以利用下个链路密钥对于网络相关数据信息进行科学解密，重新进行数据传输。通常本项数据加密技术在将数据传送到目的之前，通常每条数据信息需要经过多个通信链路的传输，因此，操作过程中应谨慎。一般在使用本项技术中，数据信息均应遵循的流程是先加密，后解密，之后重新加密，如此循环直到消息顺利传输到目标位置。计算机网络通信传输所有链路数据是依照密文开展的，链路加密对于信息传输的信息起点以及终点被掩盖，实现信息的有效加密，保障信息运行更加安全[2]。

（三）用户权限设置

用户在入网进行访问控制过程中，要合法登录到计算机服务器，并得到相关计算机资源，就对网络用户入网方式实施科学控制，入网方控制可分为对用户口令辨识与识别用户姓名，增加网络安全。加强权限设置，可在一定程度降低计算机系统产生安全故障概率。应对信息实施科学有效保护，通过数据加密技术，并使用密钥方式，对计算机网络进行安全防范，使得部分人群的计算机安全意识提升。也可在计算机网络中加强对不同管理技术充分利用，并及时处理病毒对计算机网络导致系统安全问题。

（四）节点数据加密技术

计算机运行中，节点数据加密其安全性相对较高。通常来说，这种加密技术是在计算机链路层应用，保障数据信息安全。其主要是在一定范围内发挥其潜力，利用节点数据加密技术其主要是指将数据传输到下节点解密，通常其是在安全节点快进行数据加密，并利用密钥对于计算机节点数据信息进行科学的加工处理。其属于本种传输方式与其他数据加密技术之间存在的差异，在路由器以及报头相关数据信息传输过程中，需要依照明文规定以及相关计算机网络规范进行操作。这种情况下，节点数据加密技术是无法进行运用的，这就会造成一定安全隐患。部分人员可以就会抓住此漏洞，将计算机相关数据以及信息窃取，因此，计算机网络安全人员应加强对于网络安全的定期维护，避免产生类似问题。

（五）数字签名认证技术

数字签名认证技术是一种验证计算机用户信息的方法，大体上采用加密以及解密的形式对用户的信息进行系统地验证，来保护计算机用户的数据隐私。使用数字的签名认证可以主要分为两种类型：提供数字加密以及私有数字加密。一般而言，这一技术在国家的公共以及税收行业得到了广泛地应用。主要原因是网络技术大力地促进网络支付的发展。基于这种情况，使用网络进行税收服务的人数在增加，使用网络支付付的人数也在增加。伴随网络支付技术的进步，对网络安全的需求也不断增加，并且已经采用了签名安全认证的安全措施体系，可以便于处理税收相应业务，提高税收工作成效[3]。

结束语

数据加密技术涉及的范围比较多，例如节点数据加密技术、端到端数据加密技术、链路数据加密技术等，其对于计算机网络快速运行提供很大方便，技术人员应对不同数据技术熟练操作，了解其优势以及劣势，并针对具体计算机网络情况选择合适的技术，提升技术人员的网络安全意识以及操作技能，保障计算网络信息可以顺利传递，确保数据传递更加安全。

参考文献

[1]何文海,信佳佳.网络信息安全中存在的问题及数据加密技术研究[J].网络空间安全，10（01）:28-30.

[2]杨继武.浅谈计算机网络信息安全中的数据加密技术[J].中国管理信息化，22（06）:157-158.

[3]周悦.计算机网络信息安全中数据加密技术应用研究[J].电脑知识与技术，2019（18）.