数据加密技术在计算机通信网络安全中的应用

许中堂　张武平
北京中网华通设计咨询有限公司　陕西西安　710065

摘　要：现如今，科技发展迅速，网络通信成为最主要的通讯手段。在网络通信的过程中，存在很多安全隐患，如果没有采取有效的安全防护措施，很容易造成数据丢失，被损毁、被窃取、被篡改，或者被黑客及病毒所攻击等问题。所以，按照对重要数安全保护的需求，采取有效的加密技术，包括节点加密、链路加密、端对端加密等等，本文针对这些加密技术的应用进行了阐述和分析。

关键词：数据加密；网络通信；安全

Application of data encryption technology in computer communication network security

Zhongtang Xu, Wuping Zhang
Beijing Zhongwang Huatong Design Consulting Co., Ltd. Xi'an, Shaanxi 710065

Abstract: Nowadays, with the rapid development of science and technology, network communication has become the most important means of communication. In the process of network communication, there are many security risks. If no effective security protection measures are taken, it is easy to cause data loss, damage, theft, tampering, or being attacked by hackers and viruses. Therefore, according to the requirements of important data security protection, effective encryption technologies are adopted, including node encryption, link encryption, end-to-end encryption, and so on. This paper expounds and analyzes the application of these encryption technologies.

Keywords: data encryption; Network Communications; security

引言：

随着我国科学技术的飞速发展，计算机技术作为一项至关重要的技术，逐渐走进了人们的生活。伴随着信息时代的来临，计算机通信网络的使用频率不断攀升，在此情况下，计算网通信络安全日趋突显，为促进计算机通信网络的安全发展，应采取科学的技术手段来解决计算机通信网络中的信息安全问题，确保数据顺利地被传输、存储等，为数据加密技术的运用提供科学的指导。

1. 数据加密技术概念分析

数据加密技术是指网络用户在网络通信系统运行过程中数据运输的明文数据，通过科学的计算方式对现有的数据进行合理的加密，进而实现加密传输的过程，有效防止外来危险的入侵。在此过程中借助以媒介为转换的密钥方式对现有的网络信息进行合理的加密处理，通过相关密钥获取加密后的内容以此保障网络信息的安全。

大数据时代背景之下，人们摄取消息的方式从传统的单一渠道转化为多元化的智能方式，因此在计算机网络环境运行过程中，社会大众更加关注网络安全的问题，计算机网络通信技术在不断的更新与变革过程中，对现有的数据信息内容进行合理的安全优化。提升网络信息技术人员的综合素养，使其充分掌握网络加密技术的性能、概念以及构成，进而通过充分协调相关技术，确保网络通信的安全性。

2. 安全现状

随着技术的发展和完善，计算机网络通信的优越性日益凸显。网络通信具有开放、共享、复杂、不可知等特点，受到这些因素的影响，网络通信安全也存在很多问题。尤其在开放性的特点下，经常会出现非授权访问、数据破坏、病毒攻击、线路窃听等问题，造成信息丢失、隐私窃取等重大危害。调查显示，全球范围内，平均20s就会出现一起计算机入侵事件。在互联网环境中，超过1/3的防火墙会被突破，甚至于银行、行政机关等大规模

且技术先进的机构也无法幸免。虽然，近年来人们越来越重视网络信息安全，并且采取了很多安全技术手段，但依旧无法完全规避各类安全问题。严重时会造成大量的财产损失，高达数十亿元。我国网络安全也存在诸多弊端，互联网上经常会出现黑客入侵、病毒泛滥的情况，造成政府、商业、金融等行业机构出现不同程度的损失，不仅会影响经济，还会威胁到人身安全和社会的稳定。尤其在区块链技术不断发展的背景下，很多黑客利用区块链技术发起攻击，出现洗钱、诈骗等违法行为。不仅影响技术发展和数据安全，还会危害资产安全、社会稳定。根据监管情况可以看出，区块链网络、新型技术都是比较常用的犯罪手段，技术门槛较高，即使是专业的防御机构，也无法在短期内找出事件的突破口，存在调查难、取证难、溯源难等问题。在计算机网络快速发展的今天，网络通信安全一直是十分重要的问题，不仅要不断完善技术，做好安全防御也十分重要[1]。

3. 计算机网络通信安全中数据加密技术类型分析

3.1 链路加密技术

链路加密是计算机网络通讯安全中运用较为常见的数据加密技术，针对链路加密技术可将现有的网络信息环境进行合理的科学保护，在确保网络信息安全的基础上对现有的信息进行重要的传输加密，具有较强的安全性能。在此原理之下实现对数据信息的合理保护，使其在传输过程中根据数据信息的传输需求，制定完善的数据加密技术使用方案，实现对数据的严格加密。

现有的数据信息传播会根据不同的节点选择不同的传播过程而后进行相应的加密处理，与此同时加密过程无法对其进行统一的处理，要遵循现有加密需求对其进行不同的链路信息逐一加密，根据节点的需求对其进行定期的解密以此掩饰信息传输途径，提升信息的安全性。链路加密技术可有效确保信息传输过程中的安全性，通过加密技术的合理应用有效改善传统信息传输过程中所存在的诸多问题，对现有的数据信息进行合理的科学保护，推动链路加密技术在网络通信安全中的可持续性的应用。

3.2 节点加密

节点加密要求采用报头和路由信息以明文形式进行传输，为中间节点获取信息并处理提供便利。该加密技术与链路加密技术相似但不完全相同，二者都将数据链路层加密作为基础，在通信链路上提供安全传输保护措施，在中间节点解密信息然后加密。但节点加密由节点自身的安全模块完成，链路加密则采用专门的加密设备、安全模块进行加密。在节点加密技术中，消息处于加密的状态；在链路加密技术中，节点消息则呈现为明文状态。节点加密无需再进行加密，将加密系统安装在节点上。

3.3 端到端加密

这种加密方式也被称为“包加密技术”，也是较为常见的一种技术，在数据传输过程中，整体都是密文形式。但是该种加密方式与链路加密、节点加密有着显著的区别。该加密方式只有在传输以前亦或是接收以后再进行加密处理，在其他过程中不需要另外作处理。所以这种方式相比较其他两种方式更加简便，并且有着较好的稳定性，除此之外，它的应用成本也比较低，相对于节点加密，这种加密技术并不会对设备有较高的要求，并不需要设备同步，也正是这一优点，使得对网络性能影响较低。另外，值得注意的是，即便传输过程有一个节点被损坏，那么整体数据也不会受到影响。不过该方法不能掩盖数据发出点与接收点，所以也存在一定的局限性[2]。

3.4 对称密钥加密算法

对称密钥加密算法在现代社会中应用广泛，其中较为常见的要数DES，这也是此种技术的主要代表。DES分组为64位，其算法是根据数据的排位抑或是替换，来进行加密。在这一过程中，有着十分关键的一点，就是要在初始密钥中找到16个子密钥函数，使用这种算法组成明文，可以在子密钥中通过进行排列或替换来展开操作，密钥一次就能更迭16次。要想进行密钥的解密，就需要做出逆向处理。这种算法最大的优势就在于有着极强的安全性，并且加密速度也非常快，目前在各行各业中应用广泛，其中应用最多的当属商业领域。

3.5 非对称数据加密

非对称数据加密就是采用两种密钥形式，包括私钥和公钥。公钥具有公开性的特点，用户存储私钥，所以私钥具有私密性的特点。采用非对称数据加密技术保护信息安全的过程中，私钥不会公开在网络中，在接收人获取信息之后，可以利用私钥处理信息数据，避免信息在传播过程中被窃取或丢失。但在实际应用的过程中，这种加密技术需要消耗较长的解密、加密时间，需要进一步完善和改进。

4. 计算机网络信息管理中数据加密技术的实际应用

4.1 在网络数据库中的应用

在计算机网络通信中，存在着一个较为特殊的数据库，因为数据库中有着丰富的数据资源，其中重要信息

非常多，是储存数据的重要系统。正因为其作用特殊，所以在计算机管理中，数据库也是不法分子最容易攻击的对象，通过破坏电脑非法侵入，获得丰富数据资源。很多单位在设置数据库的密钥时，没有充分考虑到最重要的安全性问题，将密钥单纯设置为简单的数字、字母，那么很容易被泄露或被破译，这将给企业带来极大的损失。通过数据加密处理，能够有效地增加密钥难度，防止信息裂口。数据库作为计算机网络通信中的关键系统，通过数据加密能够让多个密钥充分保护好数据库，提高安全系数，降低信息泄露的风险。

4.2 电子商务中应用

随着信息技术的发展，电子商务已经成为一种常见的商务模式，行业中的用户信息内容较多，与用户隐私有很大的关联性。所以，要采取有效的加密保护措施至关重要。应该采用数据加密技术来保护买卖双方的隐私信息，采用多种安全标准，对双方身份进行验证，避免隐私信息被窃取或窥探，保障商业往来的安全性。针对区块链技术为基础的黑客行为，要采取有效的链上风险防控措施。针对新型技术犯罪手段，要从物理层、数据层、加密层等多个层次入手，构建立体、多维的防护体系，新技术监管是当前最主要的发展方向。采用有效的安全工具，对分布式网络的数据存储、传输和应用等方面实施安全保护。区块链技术应用领域在不断扩大，从原本的金融延伸到供应链、工业制造等多个领域，必须要进一步加强规范和监管。针对黑客事件，要不断地反思和研究，不仅要加强法律规范与监管，还要研发更加有效的安全防护工具[3]。

4.3 推广节点加密与链路加密技术

节点加密技术与链路加密技术的科学性能相对较为复杂，在通信链路基础上对现有的传递信息进行合理的加密操作，使其在最终链路传递过程中以密文的形式呈现在社会大众面前。因此在加密过程中首先需对计算机网络安全运行现状进行细化分析，结合应用层用户程序透明的特征，对现有的数据信息运行现状进行合理的整改。制定完善的科学整改制度，在用户数据链路层断裂时运用创新型的连接方式恢复原始数据，通过节点加密技术对原始数据进行逆加工的相应处理，使其在发送端发送出符合用户运转需求的数据信息。

结合应用层自身与接收端之间的数据运行需求，在破解其加密过程中采取数据链路层的创新改革方式，对链路层的节点进行统一加密，使得链路层在数据传输过程中提升自身的安全性能，接收到安全的信息后再进行后续的解密处理。除此之外，根据不同密钥的信息传输渠道的差异性对其进行合理的节点加密，但在此过程中为通信链路的信息截取留下了较大的安全隐患。因此在计算机数据通信安全创新改革的基础上合理应用数据节点的加密技术，有效提升数据信息传输的安全性，为后续计算机网络安全的运行提供完善的发展空间。

5. 结语

综上所述，随着技术的发展和不断完善，网络通信安全逐渐受到威胁，各类安全问题层出不穷。针对各种安全隐患，需要采取有效的加密防护措施，包括链路加密、节点加密、对称信息加密等等，不同的加密方式应用场景不同，可以根据具体的使用需求进行合理选择。

参考文献：

[1]陶彩栋.大数据时代计算机网络信息安全分析：评《计算机网络安全技术》[J].热带作物学报，2021，42（10）：3095.

[2]亢婉君.数据加密技术在计算机网络信息安全中的重要性与应用[J].无线互联科技，2021，18（20）：80-81.

[3]候倍倍.计算机网络通信安全中数据加密技术的应用研究[J].电脑编程技巧与维护，2021（9）：164-165.