数据加密技术在计算机网络安全中的运用

苏东楠[1] 吴 斌[2] 孔凯薇[3] 霍学鹏[4]
北京计算机技术及应用研究所 北京市 100854

摘 要：随着互联网技术的发展，当前社会已经步入互联网时代，计算机网络技术广泛应用于社会各个领域，为人们的生活和工作提供了诸多便利。与此同时，计算机网络的应用中引发了各类安全问题，如数据信息泄漏、病毒入侵等。为有效保障计算机网络安全，需要借助数据加密技术来进行计算机网络安全保障，数据加密技术具有种类多样、隐私性强的特征，能够有效处理计算机网络数据的安全性问题。文章针对计算机网络安全数据加密技术展开论述，探索其应用策略，应用数据加密技术来推动计算机网络技术的发展。

关键词：计算机网络；数据安全；数据加密技术；互联网

引言：网络技术的普遍运用改变了人们生产方式，极大地便利了人们的生活，促进了社会的整体进步。但网络世界并非尽善尽美，各类漏洞的出现被别有用心之人利用，并以此谋取利益。不仅如此，网络时代的到来也为信息的存储与传输提供了便捷的渠道，但大数据自身所具有的高价值性也使个人信息的泄露愈演愈烈，黑客通过盗窃相关信息牟利，严重威胁着网络安全，损害网络用户利益。因此，必须在计算机网络内应用数据加密技术并不断改进，以确保网络中的信息安全[1]。

1 计算机网络安全的基本概述

我们认知中的计算机网络安全宏观上可分为四方面：（1）设备安全。这是信息系统的物质基础，是系统安全的首要问题，包括了硬件和软件设备。（2）数据安全。核心是采取措施避免数据的泄露，防止未授权用户的篡改和毁坏。（3）行为安全。是从主体行为的过程和结果来考察是否会危害网络、信息的安全。（4）内容安全。即信息安全在政治、法律、道德层次上的要求，是语义层次的安全。设备安全主要在于设备的可用性、稳定性和可靠性，而其他三方面通常具有安全性、秘密性和完整性。安全性，主要分为硬件、软件两大类安全问题，如信息设备故障、操作系统漏洞、恶意软件威胁等。秘密性，主要体现在数据不被未授权者知晓的属性，是对静态存储和动态传输的数据进行加密，是网络维护的首要手段。完整性，在行为的过程和结果中保证数据的正确、真实、未被篡改。

2 数据加密技术的相关概述

2.1 数据加密技术

数据加密技术是信息数据安全的重要技术，其原理主要是根据密码学相关技术对信息数据进行加密、解密、识别等处理，将明文数据信息借助加密算法转化为密文，数据信息的接收者使用解密密钥或解密功能将加密的数据信息恢复为原始数据消息，这有利于提高计算机网络系统中数据传输的隐蔽性和安全性。当黑客侵入电脑系统，数据会因没有解密密钥而无法知悉信息本身的内容，达到保护数据，加强电脑的安全性的目的。目前数据加密技术主要有对称加密、非对称加密、链路加密、端对端加密、节点加密等。

2.2 数据加密算法

数据加密算法分为MD5算法、DES算法、MES算法、RSA算法。MD5算法是以128位数为主的算法，这种算法首次提出是在1992年，其工作原理是，在发布文件之前以MD5算法进行加密，然后以文本为媒介生成相关的MD5数值，计算机网络安全中运用这种算法的目的是防止数据被篡改、泄露。这种算法是信息摘要类算法，此外还需要确定接收方的信息是否安全，安全的情况下才可以输入MD5值，最后还要查看一下数据的一致性，这也是为数据安全上双保险，如果查看结果不一致，就表示文件被修改，这是目前数据网络中常用的方法。而DES算法主要是先将网络信息加密变成64位秘密电文，接着还可以进行8位密文的检测或者奇数偶数检验，这就是数据加密的过程，此过程具有迭代性。MES算法相对来说比较稳定，加密效果也更为显著，该算法通过将数据明文首先输入到IP，最后转移到64位密文，这种算法目前在信息秘密解锁或者信息加密中被广泛运用。最后RSA算法主要由两个密钥组合而成，它是目前业界公认的最权威、最安全的算法。目前在计算机网络安全技术中，RSA算法运用较为广泛。为了生存密钥，首先需要随机找两个质数，质数越大安全性越高，接着将两个数进行相乘，得到乘积n，计算n的欧拉函数，最后通过欧拉函数的结果，得到了用于加解密的公私钥对[2]。

3 数据加密技术在计算机网络安全中的应用意义

3.1 杜绝网络信息的篡改

黑客入侵网络可以利用数据存储中存在的漏洞恶意篡改网络数据内容，导致网络信息传输过程中出现数据失真的严重后果，导致网络用户信息安全受到极大威胁。数据存储面临的安全漏洞同时也是威胁计算机安全的漏洞类型之一。 这类漏洞会严重影响计算机信息存储的能力，威胁到计算机内存储数据的安全。造成这种不良后果的因素有很多，一是由于相关技术人员在日常工作中忽略了数据存储安全，人为疏忽导致了信息数据的丢失。二是计算机硬件的更新迭代落后于实际需要，导致硬件环境处于风险隐患中，对计算机工作环境的安全造成了极大威胁。但数据加密技术在网络用户中的普及可以显著提升计算机信息存储的安全性能，避免黑客入侵网络，保护数据信息远离非法篡改。

3.2 有助于提升信息处理能力减少成本

数据加密技术在计算机网络安全中的运用，有助于强化计算机网络系统的信息处理能力，能把成本降到最低。首先，数据加密技术从实质上来观看，它是现今最前卫的一种科学技术，运用在计算机网络系统中，能高效提升数字信息的处理效率，同时也能完善网络技术资源，减少网络运营整体成本。其次，数据加密技术在提升计算机网络信息处理效率，同时还能确保网络系统的稳固运营，有助于优化以往技术中的缺陷，实现网络技术实施的逐步完善。最后，我国以往的计算机网络技术与现今数据加密技术相较，数据加密技术在数字信息处理层面更加的精确。所以，该技术在最大限度上能有效节省数据处理时间，节省物理、财力及人力，最后实现网络运行成本的全面降低。

3.3 阻止访客的非法访问

在计算机系统中，如果缺乏严格的授权访问控制设施，就会常出现网络数据伪造的情况，不仅会侵犯计算机用户的隐私，同时也无法保证用户的信息安全。网络具有独特的开放性和信息共享性，这也导致了木马等计算机病毒会通过网络系统进行大肆传播，这些计算机病毒大多来自非法黑客对网络安全的恶意破坏。 计算机病毒一旦植入网络系统就会表现出飞速传播和自我复制的特点，这无形中增加了在网络中实现病毒彻底消除的难度，也很难排除计算机网络的安全隐患。 除木马等计算机网络病毒外，网络硬件的存储故障同样对信息安全存储与传播造成了严重威胁。存储故障将导致计算机失去查找存储数据的功能。为防范数据丢失，避免恶意篡改数据，在这一阶段，网络安全防护通常包括对网络数据进行加密处理、设置网络防火墙和实现网络访客身份的自动识别等核心网络技术。 网络安全防护为网络提供了严密的安全保障，有效防止非法访客未经授权进入网络。

4 计算机网络安全的影响因素

4.1 操作系统隐患

硬件作为计算机组成的基础也面临着极大的风险，如处理器硬件自身漏洞越来越多，系统由多个供应商的不同软硬件拼装而成等，而物理网络互联设备作为信息传输的重要节点，往往存储着关键信息，且容易被攻击者利用、入侵。操作系统作为计算机网络系统运行程序和软件运行的前提，是计算机网络安全的基础。而现阶段计算机网络操作系统在技术层面上做的努力仍然达不到满意的效果，在计算机系统日常的运作中，常常能够发现大量系统漏洞，而这些漏洞是计算机病毒入侵用户的通道也是攻击者实施攻击的重要途径。攻击者在确定攻击目标后便会对其系统漏洞进行仔细地扫描和挖掘，以便打开缺口进一步开展攻击，这样势必会导致用户的计算机系统丢失重要信息甚至数据被恶意篡改。所以，在网络维护中，必须要重视系统漏洞的修补和防范。

4.2 病毒入侵

计算机网络当中也会出现一些病毒，即不法分子为了获取利益而设计的病毒。病毒会通过计算机网络漏洞入侵系统，并潜伏在系统当中，在获取相应指令后破坏用户的计算机。相比于其他影响因素，病毒具有传染性、潜伏性及破坏性等特点，会对网络安全造成较大影响。常见的病毒有木马病毒、蠕虫病毒及脚本病毒等，不仅会盗取网络系统内部的数据，也会导致系统瘫痪。

4.3 黑客入侵

据统计分析，计算机存在的最大安全问题，实际上是黑客入侵问题，黑客主要是心怀不轨者聘用大量的高级计算机工作者盗取计算机的内部信息。由于黑客带来的网络威胁，将会导致很多计算机业务爱好者受到好奇心驱动进而转化到有组织的团队进行黑客攻击行为，因此工作人员需要创建比较可靠的网络安全防御管理体系。

5 数据加密技术在计算机网络安全中的应用分析

5.1 对称加密技术的应用

对称加密技术指的是对信息数据进行统一密钥加密，数据加密和解密都是利用同一密钥进行处理，存在一定的对称性，因此被称为对称加密。对称加密技术是计算机网络安全中应用最广泛的数据加密方法，主要包括 AES，IDEA 和 DES等3种常用的加密算法。DES算法是数据加密技术最常规的算法。该算法结合替换、代数等加密技术，将信息分为 64 位块大小，使用 56位密钥，

迭代 16 轮加密算法。一般来说，对称加密技术具有广泛的应用范围，具有良好的应用效果，并且在加密速度方面具有显著的优势，适用于复杂、较长的信息数据加密工作。但对称密码存在以下问题:不能秘密分配密钥，缺乏自动检测密钥泄露的能力。假设网络中每对用户使用不同，密钥总数随用户数量增加而迅速增加，消息确认问题无法解决，并且单一的密钥较容易在传输中出现泄露、窃取等风险。因此，在对称加密技术应用中，要妥善保管密钥，避免出现人为的泄露等问题，发挥对称加密技术的快捷、便利优势。

5.2 非对称加密算法的应用

在通过非对称加密算法进行网络传输数据加密处理的过程中，应用到的密钥通常是一对，其中的一个密钥为私钥，另一个密钥为公钥。这两个密钥都可以对网络中传输的数据进行加密和解密处理，但是这种加密和解密处理必须建立在公钥与私钥为相对应的一对密钥的基础上才能够实现。具体应用中，公钥可以在企业内部公开，但是私钥必须通过个人进行保管，其密码一定要做好保密管理。公钥与私钥之间的重要区别在于公钥可通过网络进行传输，而私钥只能在接收到加密的信息之后再进行解密处理。通过这样的方式，就可以让网络数据在传输中获得双重保险，进而实现其安全性的显著提升。具体应用中，该加密算法的主要流程包括以下的几个方面：第一，在数据发送方与接收方之间建立起通信之前，需提前进行一对密钥设置，其中的一个用作公钥，另一个用作私钥。第二，接收方需要将公钥告知给传输方，在获得了公钥之后，传输方便可借助于这个公钥来进行信息数据的加密。当接收方接收到传输的密文后，用对应的私钥进行解密，即可得到相应的明文。第三，在数据传输的过程中，不论是传输数据的一方还是接收数据的一方，都需要进行相应的私钥设置，并做好私钥的加密处理，保证私钥不被泄漏，保证数据传输的安全性。

5.3 节点加密技术的应用

利用对数据路径进行加密的方法可以实现对个人计算机系统和互联网信息系统的安全保障，这既是节点信息加密的基本原理，同时又是节点信息加密的优点。 通过节点信息加密的使用，则可以实现对文本信息数据在传输之前就实现了加密，并同时以密文的形式进行了文件信息的传送。同时，在传输前就实施了数据加密还可以增加网络黑客的信息识别难度，提升传输环境的安全性。

5.4 端到端加密技术的应用

端到端加密技术主要是工作人员在数据传输的过程中使用加密算法加密处理信息，在数据信息并未达到预期规定的节点设备时不可以进行解密处理，这能够大幅度提升计算机网络信息的安全性。与其他加密技术相比，端到端加密技术的成本价格比较低，不但适合运用在互联网环境中，而且适合应用在局限网环境中，整个加密设计比较简洁，防止使用者在运用加密技术期间受到不良影响，端到端加密技术可以切实满足绝大多数客户的使用需要，是现在被广泛使用的加密技术。

5.5 链路加密技术的应用

链路加密技术对信息数据传输通道中各个节点进行加密，对每两个节点的信息数据进行加密、解密操作，从而保障信息数据的传输安全。这样的加密方式也被称为在线加密。在数据传输过程中会产生多个密钥，提高密钥破译难度让数据始终处于加密状态，有利于高度机密文件传输，安全系数较高。但该技术因为整个信息数据传输一直处于加密、解密过程，也增添了网络性能和管理负担，对每个节点的网络性能都会造成较大的考验。

结束语：现如今，计算机技术已经成为人们日常工作、生活中不可或缺的一部分，需要利用计算机传输的信息数量逐渐增多，但是也带来很多威胁。工作人员需要结合计算机网络信息的安全管理需要，选择合适的加密技术，对数据信息进行加密管理，这样能够有效提升计算机网络的安全性。

参考文献：

[1]刘述木，牟丽莎，杨建. 数据加密技术在计算机网络安全中的运用[J].缔客世界，2020.6（8）：39.

[2]李文杰. 计算机网络安全中数据加密技术的运用研究[J].电子制作，2021（6）：88-89，92.