数据加密技术在计算机网络通信安全中的应用

萧世昌　江志晃
广东培正学院　广东省　广州市　510830

摘　要：当代社会，互联网飞速普及，科技不断发展，已经迎来了全民互联网时代，在网络通信进程中，为确保数据的安全性，数据加密技术被普遍运用。因此，本文重点分析了在计算机网络通信安全中如何运用数据加密技术，以供参考。

关键词：计算机网络通信安全；数据加密技术；应用

1 计算机网络通信与数据加密技术概述

计算机网络通信如我们日常生活使用所见，是通过物理线路之间的连接形成数据链路，为人们提供服务的一种形式。链路之间独立工作，互不影响，但是形成了一种统一的机制和协议，通过这种网络协议，计算机网络数据进行传输和接

收。网络协议对其传输代码、程序和速率具有规范作。为了保证计算机网络的安全，需要在运行过程中采用计算机网络加密技术。所谓加密技术，是保证通信网络中，信息的交流与传输均需要通过数据来完成，通过设计在原有数据基础上进行加密，保证只有使用者才可以使用，极大的降低了数据被盗的可能性。秘钥的原理是通过数据存储和传输中的秘钥设置和解密的方式来获得使用权，接收方需要使用相应的密码才能获得明文数据，从而保证了信息传输安全[1]。

2 威胁计算机网络通信安全的关键因素

第一，黑客。黑客是计算机网络通信安全的最大威胁，电脑黑客在计算机信息安全中备受关注，这种安全隐患主要是指直接利用公共通讯网络（比如，电话系统和网络系统），入侵计算机安全系统的人，在没有经过允许的情况之下，导致计算机的稳定运作受到破坏。每一个人的电脑都会存在或多或少的安全漏洞， 如果这些漏洞直接被破解，就会使得电脑的系统失去稳定，同时无法实现正常运用。黑客可以直接读取电脑中的所有信息，导致电脑系统的稳定性和完整性无法得到保障，严重影响了网络安全和财产安全。如果公司企业的电脑办公系统受到黑客攻击，机密被窃取和泄露，就会导致公司面临巨大的经济损失，严重影响了我国的市场经济运作和商业市场的发展。

第二，病毒。病毒是计算机网络通信安全中最常见也是威胁最大的隐患。计算机病毒是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，不仅能影响计算机的正常使用，还能进行自我复制的一组计算机指令或者程序代码。 并且计算机病毒的寄生性和隐蔽性极强，病毒通常都会隐藏在其他程序或者网页之中，只有当你启动这个程序时病毒才会起到破坏作用，在此之前杀毒软件很难检测到病毒的存在。其病毒本身还有不俗的破坏性和传染性，一旦感染上计算机很难对其进行彻底清除。由于病毒往往会利用计算机操作系统的弱点进行传播， 所以，我们一定要通过掌握数据加密技术来提高系统的安全性。

第三，漏洞。网络漏洞指的是计算机中的软件、硬件，协议实施以及系统在具体运行过程中在安全策略方面上存在缺陷，从而使攻击者可以在没有得到授权的情况，对系统进行访问，甚至销毁。现阶段，计算机操作模式都支持多个进程同时运行，网络数据相互传输的目标就是诸多程序中的一个，这种操作模式在具体应用期间，容易存在安全漏洞，从而被不法人员利用[2]。黑客会抓住漏洞，对计算机进行攻击，将病毒植入到计算机中，破坏计算机系统，导致计算机无法正常运行。

3 数据安全加密技术

3.1 链路加密技术

链路加密技术作为一种加密方式，在网络信息传输维护中占据重要地位， 其安全性能非常高，其对信息传输过程地保护原理体现在以下方面。信息为传输时已经对数据进行了加密处理，信息传播时每一个特殊的节点都有自身的传播过程， 然后再进行数据信息传输加密。并且，解密过程要分成几个不同的部分，按照解密顺序针对一一解密所有的链路信息。解密过程要考虑各节点的不同展开，这样信息传输途径才会更加隐蔽。 这样无论是信息还是其传播过程都可以实现加密，让信息存储和传输更加安全[3]。

3.2 节点加密技术

从原理的角度看来，节点加密实际上与链路加密具有较强的互通性，一些基本工作的原理是具有相似之处的。在载体方面，同样也是采用链路，也同样是进行二次加密操作。但是比较特殊的是节点加密需要以明文的方式进行展现，其应用的对象一般为安全模块，因此也就造成了安全性能较低，很容易出现被破解的情况。

3.3 端到端加密技术

端到端加密是将传输点与接收点进行中，均采用秘文输入的形式，是在传输之前就对数据进行加密，但是在传输过程中无需在对数据进行加密和解密处理， 直到数据传输到使用端，由使用者对密文进行解密，获得信息。端对端具有一定的优势，在设计上，不会犹豫节点的信息被盗取而影响整体的安全性，并且设计较为简单，使用者对数据的保护到位，成本不高，能够被使用者接受。对于设备的同步性的要求也不高。但是对于通过木马攻击传输点和接收点，依然容易造成信息的丢失。因此，从技术上还需要进一步的改进。

3.4 对称数据加密技术

对称式数据加密在网络通信安全防护中的应用非常广泛。这种方式操作简单， 且效率较高。使用对称数据加密方式进行加密时，加密和解密过程中都用到同一个密钥，若想实现对数据的安全保护，就要对相关数据信息作出一定程度上的加密处理，以防一些重要数据在传输过程中被窃取。这种同一密钥技术方式，极大地减小了对信息处理的时间，使安全性有了很大提升。但对称数据加密方式在密钥管理方面存在一定缺陷，密钥的安全性无法得到保证。

3.5 非对称数据加密技术

相比于对称性加密技术，非对称加密方式在对数据进行保护时采用了两种不同密钥，分为公钥和私钥。公钥有一定的公开性，私钥是由用户保管，有很强的保密性。使用非对称数据加密技术，由于私钥不会在网络上传输，当接受方接受到信息后，利用私钥对数据进行解密，这样能避免密钥在传输过程中的数据丢失。 但非对称加密方式需要耗费更多的时间，且加密和解密都比较缓慢，因而也需要作出进一步改进。

4 数据加密技术在计算机网络通信安全中的实际应用

4.1 在局域网中的实际应用

如今，很多企业都会选择设置局域网的方式，保护自身内部信息安全。局域网加密工作能够保障企业信息安全，营造良好环境， 确保企业能够正常运转。 局域网对数据加密技术的应用，很多情况下都是用于会议的召开与资料的传输。通过提高数据保护力度，可减少外界黑客对信息的影响。局域网对数据加密这项技术的应用主要体现在传输数据时，数据会被保存在企业路由器或公司路由器，因公司路由器通常有加密功能，此时企业或公司内部路由器就可以传输这些加密文件。加密文件到达对应位置后，接收路由器就会解密，转换其中的重要文件与材料，交付给使用者、接受者，很好地避免了文件资料泄露的发生。数据加密技术在公司局域网中的使用对于提高企业竞争力与企业经济利益都有非常凸出的成效[4]。

4.2 在计算机软件中的实际应用

随着我国电子计算机网络通信用户数量的不断增加，不乏有很多恶意分子窃取网络通信用户数据。现代用户的电子计算机软件系统，经常遭受病毒或者黑客的攻击。因此，加强数据加密技术在电子计算机软件中的实际应用，对确保网络用户的网络信息安全有极其重要的保障作用。数据加密技术在电子计算机软件系统的实际应用过程中，可以选用最先进的加密方式。网络用户使用电子计算机软件系统时，只需输入密码就能有效运行软件系统，从而全面保障用户数据安全， 从根本上规避用户个人数据被不法分子盗取的情况。如果电子计算机软件受到安全威胁，用户能够借助检测软件系统第一时间清理病毒，进而全面保证电子计算机软件运行的安全性和高效性。

4.3 在电子商务中的实际应用

在计算机网络通信技术推动下，电子商务发展十分迅速，取得了巨大成就， 为推动社会经济发展做出巨大贡献。在电子商务活动开展中，必须借助于计算机网络平台支持，同时电子商务会涉及到各方利益，如果出现信息数据安全问题， 会导致很多商业信息泄露，对电子商务从业者的经济利益造成损失。因此，电子商务活动实施中需要加强对用户身份认证信息、个人资料数据等的保护，保证整个电商交易的安全。数据加密技术在电子商务中应用，能够解决这一问题，如用户在交易网站上购物过程中，数据加密技术的使用，账户登录密码和付款密码不能一样，有效保护交易安全。

4.4 在网络数据库中的应用

计算机网络通信系统运行中，数据库作为重要的子系统，作用在于能够储存海量数据资料，其自身具有较高的价值。但同时数据库也是发生数据信息安全问题的高发区，会面临数据被窃取、黑客攻击等方面的问题。

例如，黑客会利用 SQL 注入的方式入侵数据库；或者是内部人员利用自身便利侵入相关数据。一些数据库密钥较为简单，防护手段也相对较弱，一旦密钥发生泄露则会让数据库面临更

大的风险。采用数据加密技术，能够起到良好的预防措施，利用多种加密手段对数据库中数据进行保护，提升数据库整体的安全等级。

结束语

基于计算机网络通信技术的进一步发展，为人们日常生活与工作提供了便利。 虽然国内计算机网络通信技术发展时间不长，但因其发展速度较快，所以在各领域中广泛应用。针对计算机网络通信中的潜在安全隐患，有必要将引入数据加密技术，为数据信息传输与保存的安全提供必要的而保障。

参考文献

[1]钟锡珍.计算机网 络通信安全中数据加密技术的应用[J].山东工业技术，2019,(3)：153.

[2]王培屹.加密技术在计算机网络通信系统建设中的应用研究[J].轻工科技，2018,34(09):74-75.

[3]王晓楠,周婧.计算机网络通信安全中数据加密技术的应用[J].计算机产品与流通,2018(12):185

[4]叶进荣.计算机网络通信安全中数据加密技术的应用[J].信息通信，2018,186（6）:75-76.