信息时代网络安全数据加密技术研究

苏磊
（陆军边海防学院，陕西　西安　710100）

【摘　要】在信息时代，由于网络普及，数据交换日益频繁，数据安全问题愈发突显。数据加密技术作为保障网络通信和信息安全的手段，备受各界关注。本文主要研究了在网络中进行数据加密的必要性，然后分析了影响网络安全的相关内容，接下来结合计算机网络安全数据加密技术的分类，探讨了信息时代网络安全数据加密技术的实际运用。

【关键词】信息时代；网络安全；数据加密技术

探讨现代数据加密技术在网络安全中的应用，分析各种加密算法的原理及其在实际场景中的使用，才能理解网络安全的脆弱性，并寻找更加有效的保护措施应对日益复杂的网络威胁。

一、网络数据加密的必要性

随着信息化程度的提高，大量的个人隐私和机密数据在网络中传输和存储，这些数据涉及个人身份、财务信息、商业机密等敏感内容，若这些数据在传输过程中不加密就容易被黑客或恶意软件窃取、篡改或泄露，给用户带来巨大损失。对数据加密可以将其转化为一种无法被轻易解读的密文，有效保护数据隐私，这种数据只有授权用户才能解密和访问。在信息传输过程中，数据会受到木马病毒篡改或伪造的威胁，这使得数据的完整性受到破坏，接收方如果无法获得真实可信的信息，例如在电子商务中的订单信息被篡改，就会面临货物发错或是支付异常等问题，影响交易的顺利进行，使用数据加密技术就是在数据传输过程中对数据进行数字签名或消息认证等操作，防止数据被篡改或伪造，使数据在传输过程中的完整性和可信度得到保障。另外，数据加密在网络通信安全方面具有重要意义，采用数据加密技术能有效地防止数据在传输过程中被窃听或篡改，数据机密性得到保障，例如采用SSL/TLS 协议对网络通信进行加密，需要在客户端和服务器之间建立安全的通信信道，以此来防止数据被窃听或篡改。在一个信息爆炸的时代，信息的真实性成为了一个严峻的问题，利用对数据加密的方式来保护数据的真实性，使得数据的可信度上升，这对于保护国家安全、维护社会稳定、促进经济发展等都有重要意义。数据加密显然能够有效防范黑客攻击、病毒这类网络安全威胁，还可以保护个人隐私，维护用户权益，促进信息化进程健康发展。

二、网络安全分析

（一）网络漏洞

网络漏洞的种类繁多，有软件漏洞、硬件漏洞、配置错误等多种。软件漏洞是由于程序代码中的错误或设计缺陷导致的，而硬件漏洞则是因为在制造过程中的瑕疵或设计缺陷引起的，配置错误也是造成网络漏洞的常见原因，例如管理员未正确配置防火墙或更新系统补丁。网络漏洞所带来的影响广泛，对个人用户、企业机构甚至国家安全造成严重威胁，个人用户因网络漏洞就会造成个人信息被盗取或金融账户被盗用，企业机构由于网络漏洞的原因容易造成商业机密泄露或生产系统瘫痪，导致重大经济损失，而在国家层面来讲，网络漏洞如被用于网络战争或间谍活动，这直接就影响到国家的政治稳定。网络漏洞的解决难度较大，因为漏洞的发现和修复需要耗费大量时间和资源，特别是对于大型复杂系统而言，而且漏洞修复会影响系统的稳定性，这就需要在安全性和可用性之间进行权衡。

（二）病毒

病毒的传播途径很多，它可以通过感染邮件附件、下载文件、插入移动设备等多种方式传播，其中电子邮件是病毒传播的主要途径，黑客利用虚假邮件或带有恶意附件的邮件来传播病毒，一些恶意网站也通过欺骗用户点击链接或下载文件的方式传播病毒。病毒具有隐藏性和变异性，其检测和清除十分困难，有时病毒为避免被安全软件检测到，采

用加密、压缩等技术手段来隐藏自身，而且病毒还会通过变异的方式来逃避杀毒软件的检测，这就使得其很难清除干净。

（三）非法入侵

在非法入侵的手段种，黑客攻击最为常见，他们会通过密码破解、拒绝服务攻击或是 SQL 注入等技术手段来完成入侵操作，恶意软件也是常见的一类非法入侵手段，类似的例子有病毒、蠕虫、木马，它们通过感染系统来获取用户信息或控制系统。非法入侵的目的主要是为了窃取敏感信息、破坏系统功能或是获取经济利益等。由于黑客技术不断发展和演进，新型入侵手段层出不穷，使得防范变得更加困难，再加上系统和网络的复杂性使得安全风险大大增加，这也就使得发现和防范入侵变得更加复杂。

三、网络安全数据加密技术的分类

（一）对称加密

对称加密也被称为单密钥加密，特点是加密和解密使用相同的密钥，因此速度较快，适用于大量数据的加密。在对称加密中常见的算法包括数据加密标准和高级加密标准，这些算法通过对数据进行按位操作和置换，可以做到高效的加密和解密，然而对称加密存在一个严重的问题，就是密钥的安全传输和管理，因为加密和解密使用相同的密钥，所以一旦密钥泄露，就会给整个系统的安全性带来威胁。

（二）非对称加密技术

非对称加密使用一对密钥，分别称为公钥和私钥，公钥用于加密数据，私钥用于解密数据，这种方式使得密钥的传输和管理更加安全，因为公钥可以公开，而私钥只有数据的接收者才能拥有。RSA 算法是非对称加密中最为经典和常用的算法，它是基于大素数的乘法，然后利用数论的难解问题来完成安全的加密和解密。尽管非对称加密在安全性上有所提高，但由于它的计算比较复杂，所以加密和解密的速度较慢，因此一般都用于对少量数据进行加密或者用于密钥协商等场景。

（三）数字签名

数字签名是一种用于验证数据完整性和真实性的技术，它能够做到数据在传输过程中不被篡改，数字签名主要是使用私钥对数据进行加密，而验证数字签名就需要使用公钥进行解密。数字签名在网络通信、电子商务等领域有非常广泛的应用，因为它能够为数据的安全传输提供重要保障[1]。

（四）关键信息隐藏

关键信息隐藏主要是将关键信息嵌入到载体数据中，目的是隐藏信息的存在，防止被发现。这种技术基本都是用于隐写术和数字水印中，隐写术是在图像、音频、视频这样的媒体文件中隐藏信息，使得外观看起来并没有发生变化，但实际上已经嵌入了隐藏信息。数字水印是在数字内容中嵌入一些标识信息，这样可以用于证明该内容的版权和真实性。关键信息隐藏技术主要运用到信息安全、版权保护、身份验证这几个方面。

四、信息时代数据加密技术的实际运用

（一）用户个人数据的安全加密

个人数据的安全加密首要考虑的是选择合适的加密算法和密钥管理机制，在选择加密算法时要综合考虑安全和性能，一般会使用 AES 或是 RSA，这主要是因为它们具有较高的安全性和广泛的应用性，同时还要注意密钥的管理，密钥的生成、存储、传输和销毁都需要采取严格的控制措施，这样才能防止密钥泄露。在数据传输过程中采用 SSL/TLS 安全传输协议，保障数据在传输过程中的机密性和完整性，或是通过 VPN 的安全通信方式建立安全的通信通道，防止数据被窃听和篡改。在数据存储方面需要及时利用加密存储技术，将数据以加密形式存储在数据库或文件系统中，防止数据泄露，禁止非法访问。另外还要注意强化用户身份验证机制，确保只有经过授权的用户才能访问敏感数据，以此来防止非法访问和数据的泄露，同时还要结合细粒度的访问控制策略对不同用户或用户组的访问权限进行精确控制，进而最大程度地减少数据被滥用。值得注意的是，个人数据的安全加密需要全员参与，共同建立起完善的安全意识和培训机制，员工需要接受针对数据安全的培训，了解数据加密的重要性和具体操作方法，以此来提高他们对数据安全的认识，然后通过建立定期的安全演练和审计机制来及时解决潜在的安全问题，使得个人数据的安全加密措施能够持续有效地运行[2]。

（二）完善电子商务的数据加密

用户身份认证是电子商务安全的基础，结合有效的身份认证才能保障合法用户进行交易以及访问敏感信息，在用户注册和登录过程中利用多因素认证的方式来做到用户身份认证的工作，同时在对一些敏感操作和交易，要结合生物特征识别高等级身

份认证技术来进一步加强用户身份的认证。因为电子商务平台需要采用安全传输协议和加密通信技术来保障数据在传输过程中的安全性，这就可以使用公钥加密和私钥解密的方式对用户交易数据进行加密，让数据在传输过程中不被窃听和篡改，利用这些加密通信技术防止中间人攻击，降低数据泄露的风险，从而保障用户交易数据的安全。在用户交易数据存储方面，也可以结合使用加密存储技术，对用户敏感信息以加密形式存储在数据库中，防止数据被非法访问和泄露。电子商务平台需要构建完善的安全管理和监控机制，让安全管理团队负责电子商务平台的安全运维和漏洞修复，使用安全监控和审计技术对用户交易数据的访问操作进行实时监控记录，这样才能有效预防并应对安全事件，保障电子商务平台的稳定运行[3]。

（三）云服务中数据加密技术的应用

随着云存储服务的普及，越来越多的用户选择将重要数据存储在云端，如个人文件、企业数据、敏感信息。云存储服务的安全性受到广泛关注，用户的数据可能会受到黑客攻击或是被泄露。在云服务中应用数据加密技术对用户数据进行保护，数据将转化为密文存储在云端，即使数据被黑客窃取也无法轻易解密获取真实数据，这样就能有效保障在云端存储的用户数据的安全性。在云计算环境中，用户的数据需要在用户终端和云服务器之间进行传输，数据在传输过程中应用数据加密技术进行加密处理，数据在传输过程中始终处于加密状态。云服务中数据加密技术的应用还能起到对用户数据的细粒度加密管理，因为在实际应用中用户的数据具有不同的保密级别和访问权限要求，结合了数据加密技术，可以根据用户的需求对数据进行细粒度加密管理，将不同级别的数据分配给不同的密钥，以此来达到对数据访问权限的精细控制，而且只有经过授权的用户才能获得解密密钥，从而解密加密的数据，显然这样的技术使用可以很好地保护用户数据。值得注意的是，在数据加密过程中密钥的安全性非常关键，如果密钥泄露或被黑客获取就会导致安全性受到威胁，那么在云服务中就需要采用密钥管理技术对加密密钥进行安全管理。

（四）高效利用节点数据加密技术

在网络通信过程中数据需要经过多个节点的中转传输，而每个节点都可能存在安全风险，如数据被窃听、篡改或拦截，通过节点数据加密技术就能做到在数据离开发送节点之前就对其进行加密处理，保障数据传输过程中的安全性，即使在数据传输过程中被恶意节点截获，黑客也无法解密加密的数据，有效防止了数据泄露和篡改的风险。在实际网络环境中，数据传输的路径一般会发生变化，例如由于网络拓扑结构的变化或网络流量的调整等原因，在这种情况下，传统的静态加密方案无法适应动态网络环境的需求，使用节点数据加密技术可以根据实际情况动态调整加密策略，并对数据传输路径进行动态加密管理，数据在传输过程中始终处于加密状态，这样有效提高了数据传输的安全性。另外由于不同用户或系统具有不同的数据访问权限，有些只有只读权限，而有些有读写权限，利用节点数据加密技术来将不同的访问权限与加密密钥进行关联，做到对数据访问权限的精细控制和管理，在具有相应权限的用户或系统下才能获得解密密钥，从而解密加密的数据，这就保障了数据只被授权用户访问。值得注意的是，节点数据加密技术还可以结合密钥管理技术来做到对加密密钥的安全管理，在数据加密过程中密钥的安全性非常重要，若是密钥泄露或被黑客获取，加密数据将受到被泄露或篡改的威胁，因此节点数据加密技术需要采用密钥分发、密钥更新或是密钥轮换的技术手段来对加密密钥进行管理。

结语：

综上所述，在信息时代，加强对网络安全数据加密技术的研究是为了能够更好地应对网络安全领域的挑战。数据加密技术能够保障个人隐私和企业数据安全，而且也可以更好地构建安全可靠的信息社会。重视数据加密技术的创新，提升其安全性，才能够为网络安全提供更加坚实的防线，同时也需要加强国际合作，共同构建和平安全、开放合作的网络空间，实现信息化时代的共同发展。

参考文献：

[1] 李荣，夏天勇，张琪等 . 论数据加密技术在计算机网络安全中的应用 [J]. 网络安全技术与应用，2024，(01)：24-25.

[2] 王玉苹 . 论计算机网络安全中数据加密技术的应用 [J]. 电脑编程技巧与维护，2023，(10)：166-169.

[3] 张广才 . 数据加密技术在计算机网络安全中的应用意义 [J]. 网络安全技术与应用，2023，(06)：30-32.