计算机网络信息安全防护体系下数据加密技术的应用

王威宇
内蒙古自治区大数据中心　内蒙古 呼和浩特　010011

摘　要　在新时代的数字化技术全面普及的大背景下，计算机网络成了信息传递、保存和分享的主要手段，各种网络业务、政府政务服务、商业运作以及个人生活场景都深深嵌入到网络信息系统当中。网络空间的开放性、互通性使海量数据时刻处在非法窃取、篡改、泄露和滥用的安全风险之下，传统的单个安全防护手段已经不能适应复杂多变的网络安全威胁环境了。数据加密技术属于计算机网络信息安全防护体系中的关键核心技术手段，它会对原始数据实施转化处理，从而创建起数据传输和存储的安全屏障，从根本上守护住网络数据的完整程度、保密状况以及可用情况。

关键词　计算机网络；安全防护；数据加密技术

Application of Data Encryption Technology in the Computer Network Information Security Protection System

Wang Weiyu
Inner Mongolia Autonomous Region Big Data Center, Hohhot 010011, Inner Mongolia, China

Abstract　Against the backdrop of the comprehensive popularization of digital technologies in the new era, computer networks have become the primary means of information transmission, storage, and sharing. Various network services, government administrative services, commercial operations, and personal life scenarios are deeply embedded in network information systems. The openness and interconnectivity of cyberspace expose massive amounts of data to security risks such as illegal theft, tampering, leakage, and abuse at all times. Traditional single security protection measures can no longer adapt to the complex and ever-changing cybersecurity threat environment. Data encryption technology is a key core technical means within the computer network information security protection system. It transforms raw data, thereby creating a security barrier for data transmission and storage, and fundamentally safeguarding the integrity, confidentiality, and availability of network data.

Key words　Computer Network; Security Protection; Data Encryption Technology

网络空间的互联互通性冲破了信息流传的时空束缚，明显加快了社会数字化运转的速度，不过也使得网络安全隐患表现出多样化、隐蔽化、常态化的趋向。网络攻击手段的不断更新，致使数据泄露、网络入侵、信息篡改等安全事件时有发生，既会对个人信息权益造成损害，也会对企业的经营、政务运转以及社会网络安全秩序造成严重的影响。计算机网络信息安全防护体系的建立和完善，是抵御各种网络安全威胁、规范网络数据运行秩序的根本保证，数据加密技术属于防护体系的重要组成部分，它直接影响到网络数据的安全防护级别。

1　计算机网络信息安全防护体系下数据加密技术的应用原则

1.1 安全性、实用性相结合的原则

计算机网络信息安全防护体系的核心建设目标是全方位保障网络数据安全、稳定、有序地运行，所以数据加密技术的第一个应用原则就是安全性优先，在此基础上考虑技术落地的实用性。安全性原则要求数据加密技术的应用要符合网络防护体系的安全标准，对网络数据全运行流程建立闭环防护机制，用科学的加密算法、密钥配置方式，杜绝数据被非法破解、窃取、篡改的可能性，有效抵御各种常态化网络安全攻击，保证网络核心数据绝对安全[1]。在保证安全底线的基础上，还要考虑技术应用的实用性，不能因为追求加密强度而降低计算机网络运行速度和用户的使用体验。网络系统传输的数据量大，交互复杂，在保持加密技术高效的同时，不引起网络传输卡顿、数据处理缓慢、系统负载过大等问题，满足各种网络环境、不同数据类型的使用要求，简化加密操作过程，降低技术实施的门槛，使高强度加密和高效的网络使用达到相互促进的效果，发挥数据加密技术在网络安全防护体系中的实战作用。

1.2 适配性与动态性相融合的原则

计算机网络信息安全防护体系具有整体性、系统性特点，内部包含各种类型的网络设备、运行系统、防护模块以及数据类型，运行环境复杂且存在明显的差异，因此数据加密技术的运用要遵照适配性和动态性相统一的原则。适配性原则要求加密技术充分契合网络防护体系的全部架构，适应各个层次的防护需求，对公开数据、私密数据、核心涉密数据等不同的数据种类，采用相应的加密方式和加密强度，并且可以兼容各种网络传输协议、存储设备和业务系统，防止由于技术适配性不够而造成防护漏洞、系统冲突等状况的发生，使加密技术与整个防护体系紧密结合在一起。动态性原则是根据网络安全威胁的迭代特性提出的，网络攻击手段、入侵方式处在不断更新变化之中，固定一个加密模式很难适应安全环境的变化。这就需要数据加密技术具备动态调整的能力，根据网络运行状况、安全风险等级、业务场景的变化不断改进加密算法、更新密钥体系、改变加密防护策略，持续填补网络安全防护短板，使加密防护能力一直跟上动态变化的网络安全环境，保证网络信息安全防护体系的长期稳定运行。

2 计算机网络信息安全防护体系下数据加密技术的应用意义

2.1 构建网络数据全生命周期安全防护体系

计算机网络信息安全防护体系的主要防护对象是网络流通和存储的各种数据，数据安全是网络安全的核心，数据加密技术的落地应用，从源头上完善了网络数据全生命周期的安全防护机制，从根本上解决了传统网络防护重边界、轻核心的防护问题。传统的网络安全防护大多集中于网络端口、系统边界的风险拦截上，不能对数据本身起到有效的防护作用，一旦边界防护被突破，核心数据就会直接暴露在安全风险之下[2]。数据加密技术可以对数据本身发挥直接的作用，在数据采集完毕后立即完成加密转换，把原来的可读数据变成无规律、无法直接识别的加密数据，在数据传输、云端存储、终端使用全过程里，即使数据被非法获取，非法人员也读取不了、篡改不了有效的数据内容，从根本上消除了数据泄露和滥用的风险。加密技术可以和防护体系的溯源机制结合起来，对数据的操作行为进行全过程的记录，一旦发生数据安全问题，就可以迅速找到风险源，全方位地加强网络数据安全防护体系的基础。

2.2 建立完善的网络信息安全防护体系

完整的计算机网络信息安全防护体系是由边界防护、终端防护、数据防护、运维防护等多个主要部分组成，各种防护技术互相配合、互相补充，才能形成全方位、立体化的防护体系。传统的防火墙、入侵检测、病毒查杀等被动防护手段主要起网络边界风险拦截、系统漏洞查杀的作用，缺少对数据内核的主动防护模块，造成整个防护体系结构上的不足，不能达到全方位无死角的安全防护效果。数据加密技术属于主动型、内核型防护技术，很好地弥补了网络数据内核防护的空白，充实了防护体系的技术层次，使得防护体系由“边界防御”深入到“内核防护”。该技术可以和各种传统的防护技术深度结合，形成边界拦截、内核加密、全程监管的立体防护体系，改善防护体系的运行逻辑，克服传统防护模式的漏洞和不足，使计算机网络信息安全防护体系的结构更完整、功能更全面、防护更系统。

2.3 保证网络业务的正常、有序开展

各行各业的数字化业务都依靠计算机网络系统来运作，政务办公、电子商务、金融交易、民生服务等各种网络业务的有序进行，完全依靠安全稳定的网络信息环境，数据安全直接影响到网络业务的运行质量和发展的秩序。网络数据泄露、篡改、丢失等安全问题会造成业务数据失效、业务流程中断，并且还会引起交易纠纷、政务失误、用户权益受损等一系列连锁问题，严重扰乱网络业务运行秩序[3]。数据加密技术在网络安全防护体系中不断规范化地使用，可以保证各种网络业务数据的真实性、完整性和保密性，在传输交互、存储调用、共享使用等环节不会出现数据被篡改、泄露的情况，为网络业务流程的顺利进行提供主要支撑。同时可靠的加密数据可以提高网络系统的运行可信度，增加用户对网络平台、网络业务的信任度，为各种数字化业务的创新发展、规模化推广创造安全稳定的网络环境，促进各行各业数字化转型稳步发展。

3 计算机网络信息安全防护体系下数据加密技术的应用

3.1 数据传输环节加密防护的应用

数据传输是计算机网络数据交互的主要环节，也是网络安全风险高发期，网络数据在跨终端、跨平台、跨区域传输过程中很容易被非法截取、窃取和篡改，是网络信息安全防护体系的重点防护场景。数据加密技术在传输环节的应用，可以对所有的处于传输状态的网络数据做前置加密处理，从而消除传输过程中出现的各种安全风险。根据具体的网络传输场景的不同，选择相应的加密算法和传输加密方式，对于普通网络的信息传输，可以使用对称加密技术来完成快速加密和解密的操作，保证数据高速传输的同时也具备基本的安全防护功能；对于政务、金融、涉密等核心私密数据的传输，可以使用非对称加密技术，利用公钥加密、私钥解密的双向密钥机制来提高数据传输的加密级别，防止传输过程中出现数据被破解的风险[4]。

同时可以将加密技术和网络传输协议结合起来，在传输通道上进行加密封装，形成专用的安全传输通道，防止数据在传输链路上被非法抓取，全方位加强网络信息安全防护体系在数据传输环节的防护能力，保证传输数据的安全。

3.2 数据存储环节的加密防护应用

伴随着网络数据量的不断增加，云端存储、服务器存储、终端存储成了网络数据保存的主要形式，大量的核心数据长时间存放在网络服务器和云端平台上，由于存储环境的开放性，数据存在着被非法访问、恶意窃取、批量泄露的安全风险，数据存储环节的加密防护成了网络安全防护体系的重要工作内容。数据加密技术在存储环节起到的是对静态存储数据全方位加密的作用，从根本上消除存储数据的安全隐患。在网络系统的服务器、云端数据库存储数据时可以进行分层加密，对普通公开业务数据使用轻量级加密，保证存储安全又节省系统资源，对用户隐私数据、企业核心经营数据、政务涉密数据等重要信息使用高强度加密，设置专门的访问密钥和权限验证机制，只允许授权人员通过专用密钥进行解密和数据调用，防止非法人员的越权访问和数据窃取[5]。

3.3 用户身份认证及访问加密应用

网络系统日常运行时，所有的用户登录凭证、身份标识、操作权限等信息都是以数据的形式在网络中存储和流转的。使用数据加密技术对用户的账号、登录密码、数字证书、生物特征密钥等重要的身份信息加以高强度加密，在传输过程中以及静默状态下都不能被黑客非法获得、暴力破解、技术伪造，从而从根本上杜绝使用非法账号登录、冒用他人身份进行攻击的安全隐患。利用已经成熟起来的加密技术框架来创建出一种灵活且安全的动态身份认证机制[6]。当用户试图访问网络系统或者申请获取核心业务数据的时候，系统后台就会用事先分发的加密密钥或者令牌，对用户的在线身份进行实时的核验和双向认证，只有验证全部通过之后，用户才能得到与其角色相符的、被严格限定的数据访问和操作权限。另外，对于系统内不同的层级、不同的责任用户，可以建立相应的加密权限管理机制，用密钥分层、权限绑定等方式来达到按需授权、分级管控、精准防护的目的。该种应用方式可以从网络访问的入口端直接拦截、过滤非法请求，有效地规范了整个网络访问秩序，它同前面所提到的数据传输加密、数据存储加密等技术手段相互配合、紧密相连，一起形成了一个多层次、纵深化的主动防御体系，使计算机网络信息安全防护体系的总体威慑力和实战防护能力得到全面提升。

4 结束语

数据加密技术属于防护体系中的主动防护、内核防护的关键技术，它渗透到网络数据运转的全部环节当中，依靠科学的应用准则、多样化的应用价值、广泛的应用场合，给网络数据安全赋予了有力的技术支撑。本文通过对计算机网络信息安全防护体系下数据加密技术安全性与实用性兼顾、适配性与动态性统一的应用原则进行系统的分析，对数据加密技术在筑牢数据安全屏障、完善防护体系架构、保障网络业务运行方面所具有的重要意义进行了剖析，并从数据传输、数据存储、身份认证和访问控制4个方面提出了具体的实施路径。

参考文献

[1]王传军.加密技术在高中信息技术数据安全中的应用[J].家长,2025(20):55-57.

[2]王桥云.量子加密防伪技术在生态环境监测数据质量控制中的应用研究[J].中国品牌与防伪,2025(7):20-22.

[3]王瑶.数据加密技术在大数据安全防护中的应用研究[J].科技风,2025(18):70-72.

[4]李小华.混合加密算法在计算机网络数据传输安全技术中的应用[J].百科知识,2025(18):14-16.

[5]孟学尧,李浩婕.基于计算机网络课程的思政教学研究与探索[J].数字通信世界.2025(11):2-3.

[6]马晟皓.基于安全视角分析计算机网络管理创新策略[J].软件,2025,46(11):161-163.

（本文编辑　曹　阳）

