网络通信中的数据信息安全保障关键技术

姚庆来
中国机械设备工程股份有限公司　北京　100073

摘　要：随着信息化时代的发展，网络信息安全直接关乎到国民经济的安全，越来越成为人们关注的焦点。计算机通信网络作为信息技术的交流平台，相应的也成为经济发展的命脉。因此，相关部门应该加大数据安全技术应用研究的力度，才能在给予计算机通信网络全方位安全保护的基础上，充分发挥自身的优势，构建完整的网络数据安全体系，推动互联网的健康可持续发展。

关键词：网络通信；数据信息；安全保障

1 网络通信安全的重要性

网络通信安全是当今信息时代中至关重要的一环。随着互联网的普及和技术的迅猛发展，网络通信已经成为人们日常生活和工作中不可或缺的一部分。然而，网络通信的广泛应用也带来了各种安全威胁和风险。第一，网络通信安全对个人隐私保护至关重要。在网络通信的过程中，存在着大量的个人敏感信息，比如身份证号码、银行账号、电话号码等。如果这些信息被黑客或犯罪分子获取，将会给个人和社会带来严重的损失和风险。第二，网络通信安全对商业机构和政府部门来说也非常重要。商业机构的商业机密、企业数据、商业合作伙伴的信息，政府部门的国家安全、公共安全等都需要得到保护。一旦这些信息泄露或被篡改，将对企业和政府造成严重的经济和社会影响[1]。第三，网络通信安全也对国家安全具有重要意义。网络攻击已成为一种新型的国家安全威胁，通过网络渗透和网络战争，黑客和犯罪分子可能获取国家机密、破坏国家基础设施、干扰社会秩序等。因此，确保网络通信安全对于国家安全至关重要。在保障网络通信安全方面，各个方面都需发挥积极作用。政府应加强相关立法和监管，完善网络安全保护体系；企业和组织要建立健全的网络安全管理制度和技术防护措施；个人也要强化网络安全意识，妥善保护个人信息。只有形成全社会共同关注和共同参与的网络安全格局，才能够更好地保护网络通信安全，确保信息时代的顺利发展和社会的稳定运行。

2 保障网络通信中数据信息安全的作用

保障网络通信中数据信息安全是十分重要的，它扮演着多个方面的关键作用：（1）保护个人隐私和信息安全：网络通信中的数据信息可能包含个人隐私、财务信息、医疗记录等敏感数据，保障数据信息安全可以防止这些个人信息被不法分子获取和利用，从而确保个人的隐私权和信息安全。（2）保障商业和企业安全：网络通信对商业机构和企业来说至关重要，保障数据信息安全可以防止商业机密被窃取以及企业关键数据被篡改或毁损，从而保证商业竞争力和运营稳定性。（3）确保社会秩序和公共安全：网络通信安全问题直接关系到社会秩序和公共安全，防范网络攻击和信息泄露等问题可以有效减少网络犯罪行为，维护社会的稳定运行和公众的安全感[2]。（4）保障国家安全：网络通信安全问题对国家安全具有至关重要的意义。保障数据信息安全可以防止国家机密被泄露，阻止恶意行为导致国家基础设施受到破坏或干扰，从而维护国家的安全和稳定。

3 网络通信中数据信息安全隐患分析

3.1 数据信息结构问题

网络通信中的数据信息安全隐患涉及许多方面，其中一个关键因素是数据信息结构问题。以下是对数据信息结构问题在网络通信中可能带来的安全隐患的分析。首先，数据信息结构的不合理可能导致安全漏洞。在设计和实施数据信息结构时，如果没有考虑到安全性因素，可能会导致数据的不完整性、不一致性和不可靠性。这些问题可能会被黑客或犯罪分子利用，从而导致数据泄露、篡改或破坏。其次，数据信息结构的复杂性可能导致错误的处理和管理。随着网络通信中数据量的增大，数据信息结构变得越来越复杂。如果没有正确的数据管理和处理机制，可能会导致数据丢失、错误处理或不当访问。这会使网络通信中的数据易于受到攻击或引发安全事故。数据信息结构的标准化和统一性问题也会带来安全隐患。如果没有统一的数据信息结构标准，可能导致数据格式混乱，数据传输错误或数据解析困难。这种情况下，攻击者可以利用这种混乱来进行数据篡改、欺骗或拒绝服务攻击[3]。最后，数据信息结构的访问控制不当可能导致安全漏洞。如果数据信息结构没有

正确的访问控制机制，可能会导致相应数据的非授权访问和使用。这将增加数据信息泄露、信息冒用和攻击的风险。

3.2 网络通信软件问题

网络通信中的数据信息安全隐患不仅涉及数据信息结构问题，还与网络通信软件本身相关。以下是对网络通信软件问题可能带来的安全隐患的分析。网络通信软件的漏洞可能会被黑客或犯罪分子利用。随着网络通信软件的复杂性和功能的增加，可能存在程序设计上的错误和缺陷，这些漏洞可能被攻击者利用，导致数据信息泄露、篡改或破坏。网络通信软件的不安全配置可能导致安全隐患。如果网络通信软件的配置没有按照安全最佳实践进行，可能会导致弱密码使用、未经授权的访问和不安全的数据传输等问题。攻击者可以利用这些漏洞来入侵系统、窃取数据或者进行拒绝服务攻击。网络通信软件的升级和补丁问题也可能导致安全隐患。如果网络通信软件的升级和补丁没有及时安装或者存在漏洞，可能会使系统容易受到已知的攻击，增加被攻击的概率[4]。最后，网络通信软件的第三方组件和插件也可能存在安全隐患。网络通信软件通常依赖于第三方组件和插件来实现特定功能，如果这些组件和插件存在漏洞或者被恶意篡改，可能会导致整个系统的安全受到威胁。

3.3 网络系统操作问题

网络通信中的数据信息安全隐患不仅与数据信息结构和网络通信软件相关，还与网络系统操作问题有关。以下是对网络系统操作问题可能带来的安全隐患的分析。人为因素是造成数据信息泄露和安全漏洞的主要原因之一。如果网络系统操作人员缺乏对安全原则和操作规程的理解和遵守，可能会导致意外的数据泄露、错误的数据处理或不当的访问控制等安全问题。弱密码容易受到猜解和暴力破解攻击，而账户管理不当则可能导致非授权访问和滥用权限。攻击者可以利用这些漏洞来获取对网络系统的控制权，从而访问、篡改或破坏数据信息。网络系统通常具有许多安全功能和控制措施，如防火墙、入侵检测系统和访问控制列表等。如果网络系统操作人员不了解或不正确地配置和使用这些安全措施，可能会导致漏洞或限制了系统的安全性能。当未授权用户恶意访问系统或有授权用户滥用权限时，可能会导致数据信息泄露、篡改或破坏。这种情况下，必须加强对用户身份验证、访问控制和操作审计等方面的管理，以降低安全隐患的风险[5]。

4 网络通信中的数据信息安全保障技术

4.1 网络用户身份验证

网络通信中的数据信息安全保障离不开有效的技术手段，其中网络用户身份验证是十分重要的安全保障技术。首先，网络用户身份验证技术可以确保数据通信的参与者的身份合法和真实性，防止未经授权的用户进行非法访问和操作。通过采用强密码、多因素身份验证和生物识别等方法，有效地确保只有经过验证的用户才能获得访问和使用数据的权限，从而防止黑客、病毒和恶意程序等对数据进行非法篡改和窃取。其次，网络用户身份验证技术能够保护用户的个人隐私和敏感信息。通过使用加密算法、安全通信协议和安全令牌等措施，确保用户在网络通信中的个人信息和敏感数据得到保护，防止它们被第三方非法获取和利用。网络用户身份验证技术还可以为数据通信提供审计和追溯功能，确保数据信息的可信度和可靠性。通过记录用户身份验证的日志和审计数据，能够追踪和分析用户的访问行为，及时发现和应对安全风险，保障数据信息安全。在实施网络用户身份验证技术时，可以采用多种方式。使用强密码来保护用户账号的安全，要求用户设置较长、复杂且定期更新的密码[1]。可以使用多因素身份验证，结合密码和短信验证码、指纹识别、声音识别等多种方式，提高身份验证的准确性和安全性。另外，网络平台可以使用安全令牌或智能卡等物理设备，与用户设备进行交互进行身份验证。也可以采用生物识别技术，如指纹识别、面部识别、虹膜识别等，通过分析用户的生物特征进行身份验证。

4.2 数据解析系统构造

网络通信中的数据信息安全保障技术在数据解析系统构造方面具有重要作用。数据解析系统是用于将加密、压缩或混淆等方式处理的数据恢复成可读取和分析的原始数据的系统。（1）加密算法和解密技术是构造安全的数据解析系统的重要组成部分。通过采用高强度的加密算法和安全的密钥管理机制，将数据进行加密处理，可以有效防止非法访问和数据信息泄露。而解密技术则用于将加密数据恢复为原始数据，以便进行后续的分析和处理[2]。（2）数据压缩技术也是数据解析系统构造中的重要技术之一。通过对数据进行压缩处理，可以减少数据的传输和存储空间，并提高数据的传输效率。同时，压缩后的数据在解析时需要进行解压缩操作，因此需要构建可靠的解压缩算法和系统，确保数据的完整性和安全性。（3）数据混淆技术也可以在数据解析系统中起到一定的安全保护作用。对于敏感的数据信息，可以采用混淆技术对其进行处理，使其在传输和存储过程中无法被轻易识别和理解。只有经过相应的解混淆操

作，才能恢复为可读取和分析的原始数据，从而提高数据的安全性和保密性。在数据解析系统构造中，还需要考虑对其他零散的数据信息进行整合和归类的技术。通过建立合适的数据模型和架构，将不同格式和来源的数据整合起来，并进行相应的标注和分类，从而提高数据处理的效率和准确性。

4.3 防火墙技术

防火墙是位于网络边界的设备或应用程序，用于监控和控制数据流量，以保护内部网络免受未经授权的访问和恶意攻击。首先，防火墙技术可以实施访问控制策略，限制进出网络的数据流量。通过在防火墙上配置访问控制列表（ACL）、规则集和安全策略，可以根据源地址、目标地址、端口号和协议等多种因素来控制进出网络的数据流量。这样可以阻止未经授权的访问和限制对网络资源的访问权限，保护网络中的数据信息安全。防火墙可以检测并且阻止各种类型的网络攻击，如入侵、病毒和恶意软件等。通过使用网络威胁情报、行为分析和签名数据库等方法，防火墙可以对网络流量进行实时分析和检测，在发现异常行为时及时采取措施进行阻断和防御。防火墙技术还可以提供网络地址转换（NAT）和端口转发等功能，增强网络的安全性和隐私保护。通过隐藏内部网络的真实IP地址和端口号等信息，可以降低网络暴露于外部攻击威胁的风险，并提供一定程度的隐私保护[3]。在实施防火墙技术时，可以采用网络硬件设备和软件应用程序相结合的方式。硬件防火墙通常是专门的设备，可以提供高性能的数据包过滤和处理能力。软件防火墙则是一种应用程序，可以在普通计算机上运行，通过软件配置和设置来完成防火墙的功能。根据实际需求和网络规模，可以选择适合的防火墙产品和解决方案。

4.4 加强对网络信息数据储存的措施

在网络通信中，对网络信息数据储存的安全保障是至关重要的。使用加密技术来保护存储在网络中的敏感信息数据。通过使用强密码和加密算法对数据进行加密，可以有效防止未经授权的访问和数据泄露。只有经过解密操作，才能访问、读取和使用加密数据，从而提高数据的机密性。采用访问控制机制来限制对存储数据的访问权限。通过设置适当的访问控制策略，只有经过授权的用户或角色能够访问和操作存储的数据。这可以包括用户身份验证、访问权限管理和审计日志等措施，以确保只有合法的用户才能够访问、修改和删除数据。备份和灾难恢复方案也是加强对网络信息数据储存的重要措施。通过定期备份数据，并将备份数据存储在安全的离线介质或云存储中，可以防止数据丢失或损坏。同时，建立完善的灾难恢复方案和操作流程，可以在发生数据意外丢失或系统崩溃时迅速恢复数据。定期的安全漏洞扫描和漏洞修复也是加强对网络信息数据储存的重要措施。通过定期检测系统和应用的漏洞，并及时修补安全漏洞，可以防止黑客利用已知漏洞入侵系统，并提高数据信息储存的安全性[4]。建立合规性与监管制度和政策也是保障网络信息数据储存安全的重要措施。根据相关法律法规和行业标准，建立合规性与监管制度，制定相关政策和规定，明确数据处理和存储的责任与义务，加强对数据安全的监管并提升数据信息储存的可信度和合规性。

结束语

随着技术的不断发展，网络攻击手段也不断进步，我们需要不断地更新和加强安全技术，以应对不断变化的安全威胁。通过综合应用多种安全技术和制定相应的安全策略，我们才能更好地保障网络通信中的数据信息安全。

参考文献

[1]范芳东,范双南.计算机网络信息安全中数据加密技术探究[J].电脑编程技巧与维护,2021,06:162-163.

[2]白红.计算机网络安全中数据加密技术的运用研究[J].电脑编程技巧与维护,2021,06:166-167.

[3]郭丰.网络通信中的数据信息安全保障技术分析[J].中国新通信，2021，23（04）：155-156.

[4]栗强,郭利,钟翩宇.网络通信中的数据信息安全保障技术[J].信息通信，2020，33(6):194-195.

[5]于鑫玥.网络通信中的数据信息安全保障技术[J].中国新通信，2020，22(4):129.