网络通信中的数据信息安全保障技术研究

廖远龙
中国移动广西公司防城港分公司　广西　防城港　538000

摘　要：现如今，我国是社会科技快速发展的新时期，网络通信系统的构建涉及较多的通信线路和交换设备，且设备服务器的连接较为复杂，为确保网络通信系统能够安全稳定的运行，往往需要过硬的信息技术来打造专门的工作模式，最大限度保证网络通信系统内部数据信息传输安全，以此来让网络通信系统处于平稳运行的状态。

关键词：网络通信；数据信息安全；保障技术

1 网络通信中的信息安全特点

网络通信在现代社会中发挥着重要作用，而信息安全则成为网络通信的一个关键问题。第一，网络通信的信息安全面临着传输风险。在网络传输过程中，信息有可能会被黑客、病毒或恶意软件攻击，导致信息泄露、篡改或被非法获取。这就要求在网络通信中采取必要的安全措施，如数据加密、防火墙等，以确保传输的信息能够安全到达目的地。第二，网络通信的信息安全具有易复制性。在网络中，信息可以以很快的速度和低成本进行复制、传播和转发，这为信息的非授权使用和盗取提供了机会。因此，在网络通信中，需要采取技术手段和法律措施来保护信息的版权和知识产权，防止信息的盗用和侵权行为。第三，网络通信的信息安全具有匿名性和虚拟性。在网络通信中，用户可以隐藏自己的身份和行踪，因此，黑客和网络犯罪分子可以更容易地进行攻击和侵入行为。为了保护网络通信中的信息安全，需要加强用户身份验证和安全凭证的使用，确保网络通信的参与者的真实身份和行为可以追溯和验证[1]。第四，网络通信的信息安全还面临着多样化的威胁和攻击手段。黑客和网络犯罪分子不断创新和发展各种攻击手段，如网络钓鱼、病毒感染、勒索软件等等，使得信息安全防御面临着巨大的挑战。为此，网络通信中的信息安全需要持续不断的技术创新和应对策略的更新。

2 网络通信安全的重要性

在现代社会中，网络通信的安全性变得越来越重要。（1）网络通信安全是信息安全的基石。随着互联网的普及和信息技术的升级，人们的个人、商业、政府等各种重要信息大多数以网络通信的形式进行传输和存储。如果网络通信不安全，那么这些重要信息就会面临泄露、篡改、盗用等风险，给个人和社会带来严重的损失和威胁。因此，保障网络通信的安全性是保障整个信息安全的基础。（2）网络通信安全对于保护个人隐私尤为重要。在网络通信中，人们经常涉及到私人的、敏感的信息，如身份证号码、银行账号、密码等。如果这些信息泄露，就会给个人隐私带来巨大的风险，并可能导致身份盗用、财产损失等问题。网络通信安全的保护，可以有效地防止个人隐私被侵犯，确保个人信息的私密性和机密性。（3）网络通信安全对于商业和金融活动的正常进行至关重要。在网络通信中，企业、组织和金融机构经常需要进行商业合作、数据交换、资金转移等活动。如果网络通信不安全，这些活动就会面临着信息泄露、商业机密被窃取、金融交易被攻击等风险。安全的网络通信可以建立商业和金融交易的可信赖性，促进经济和金融的发展[2]。（4）网络通信安全是国家安全的重要组成部分。在当今全球化的信息社会中，各个国家之间的政治、军事、经济等各个领域都需要通过网络进行通信和协作。如果网络通信不安全，国家机密、军事战略等重要信息就会面临泄露、窃取等风险，给国家的安全和稳定带来严重威胁。因此，保障网络通信的安全性对于国家的利益和安全至关重要。

3 网络通信中信息数据安全问题

3.1 网络病毒

在网络通信中，信息数据安全问题是一个不可忽视的挑战。网络病毒作为信息数据安全的主要威胁之一，给网络通信带来了严重的风险。网络病毒是一种恶意软件，它的主要目的是破坏、感染或窃取计算机上的数据和信息。网络病毒可以通过网络传播，感染到无数的计算机和设备，造成大范围的破坏和损失。它们会在计算机系统中植入恶意代码，破坏操作系统、软件和文件，甚至可以窃取个人隐私和敏感信息。网络病毒的传播方式多种多样，常见的包括通过电子邮件附件、可移动存储设备、恶意链接、社交媒体以及文件共享等渠道。一旦计算机感染了病毒，它会自动复制和传播，进一步感染其他计算机，造成信息数据的泄露和破坏[3]。

3.2 数据泄露问题

在网络通信中，数据泄露是一个严重的信息数据安全问题。数据泄露指的是未经授权或许可的情况下，敏感和机密的数据被泄露、公开或者被不当使用。数据泄露带来的风险包括个人隐私泄露、商业机密泄露、金融欺诈、恶意利用等。数据泄露可能发生在多个环节和形式中。其中一种常见的情况是网络攻击导致的数据泄露。黑客通过网络攻击和入侵，获取到存储在公司、组织或个人电脑和数据库中的敏感数据。另一种情况是内部人员的不当行为，如团队成员的泄露、商业竞争对手的渗透等。此外，还有一些外部的威胁，比如云存储服务提供商的数据泄露、恶意软件的感染，以及社交媒体等平台上的信息泄露等。

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

在网络通信中，数据信息安全保障技术和网络用户身份验证是确保网络通信安全的重要手段。首先，数据信息安全保障技术方面，加密技术是最常用的手段之一。通过使用加密算法，将敏感的数据信息进行转化，使其无法被未经授权的人读取和理解。常见的加密技术包括对称加密和非对称加密。对称加密利用同一个密钥对数据进行加密和解密，而非对称加密则使用公钥和私钥进行加密和解密，提高了数据的安全性[4]。其次，网络用户身份验证也是确保网络通信安全的重要环节。网络身份验证通过验证用户的身份和权限来控制和限制其对数据的访问和使用。常见的身份验证技术包括密码验证、生物特征认证（如指纹和面部识别）、双因素认证等。这些技术通过要求用户提供准确的身份信息或额外的安全措施来确认用户的真实身份，从而降低了未授权用户访问系统和数据的风险。网络通信中的数据信息安全保障技术还包括防火墙和入侵检测系统的应用。防火墙可设置规则，控制和监测网络通信的流量，阻止未经授权的访问和攻击。入侵检测系统则能够监测和识别潜在的网络攻击行为，并及时采取措施进行阻止和报警，保护系统和数据的安全。定期的安全评估和漏洞扫描也是非常重要的。通过对网络系统的安全性和漏洞进行评估，可以及时发现潜在的安全隐患，及时修补漏洞，从而减少安全事故发生的可能性。

4.2 防火墙技术

在网络通信中，防火墙技术是一种常见的数据信息安全保障技术，它通过设置一系列的规则和过滤器来控制和监测网络通信的流量，以阻止未经授权的访问和攻击。防火墙可以分为软件防火墙和硬件防火墙两种类型。软件防火墙部署在操作系统或特定的应用程序中，它可以检测并过滤进出系统的网络流量，根据预设规则来决定是否允许该流量通过。硬件防火墙则是一种独立的设备，通常放置在网络的边界，其主要功能是筛选和监控网络通信的流量，并对进出的数据包进行审查和过滤。防火墙通过设置规则来控制网络通信的流量。这些规则可以基于源IP地址、目标IP地址、端口号、协议类型等信息进行筛选。例如，可以设置规则只允许特定IP地址或特定域名的请求通过，或者禁止特定端口号的访问。通过灵活的配置，防火墙可以决定允许和禁止哪些网络通信，从而保护系统和数据的安全。防火墙还能够监测和记录网络通信的活动，如设备连接、数据传输等，以及检测特定的网络攻击行为，如端口扫描和恶意软件感染等[5]。当防火墙检测到可疑活动时，它会采取相应的措施，例如阻止该活动的继续进行，并向管理员发出警报。除了传统的静态防火墙，还有一种被称为“下一代防火墙”的技术。下一代防火墙不仅具备传统防火墙的功能，还结合了更多的安全特性，如应用程序识别与控制、用户行为分析、入侵防御系统等。它能够对网络通信进行更细粒度的控制和检测，提供更强大的安全性和性能。

4.3 数据安全的实现目标

首先，保密性是数据安全的重要目标。保密性要求在数据传输和存储过程中，只有授权人员才能访问和获取敏感数据。为了实现保密性，常用的技术包括数据加密和访问控制。数据加密通过将数据转化为不可读的形式，即使被非法获取，也无法读取其中的内容。访问控制则通过设置权限和身份验证机制，限制只有合法用户才能访问敏感数据。完整性要求在数据传输和存储过程中，数据不被修改、篡改或丢失。为了实现完整性，常用的技术包括数据哈希和数字签名。数据哈希是将数据转化成固定长度的数字摘要，通过比对接收到的数据和哈希值是否相符来验证数据是否被修改。数字签名则是在数据上加上私钥生成的数字标记，验证接收到的数据是否经过合法的发送方签名。可用性要求数据在需要时能够正常、及时地访问和使用。为了实现可用性，常用的技术包括备份和灾备。备份是将数据复制到其他存储介质或地理位置，以便在原始数据丢失或损坏时进行恢复。灾备则是将数据备份到远程地点，以应对自然灾害、硬件故障等导致数据中心不可用的情况。此外，认证和授权是数据安全的重要环节。认证验证用户的身份，确保其是合法的用户，而授权则是在认证成功后，授予用户特定的权限和访问范围。认证和授权技术可以

采用密码、生物特征认证和双因素认证等，以确保网络通信中只有授权用户才能访问和使用数据。

4.4 IP地址保护

IP地址是在网络中识别和定位设备的唯一标识，攻击者可以通过获取和分析目标主机的IP地址来发起攻击或侵犯隐私。因此，保护IP地址的安全性对于维护数据信息的安全至关重要。一种常见的IP地址保护技术是网络地址转换（NAT）技术。NAT技术在网络边界设备上配置，通过将内部私有网络中的IP地址映射为外部公共IP地址，从而对外隐藏了真实的IP地址。这样做的好处是，攻击者无法直接访问内部网络的设备，提高了系统的安全性。此外，NAT还可以同时实现多个设备共享一个公共IP地址的功能，提高了网络资源的利用率。另一种IP地址保护技术是使用代理服务器。通过使用代理服务器，用户的真实IP地址可以隐藏起来，被代理服务器的IP地址代替。这样做可以保护用户的隐私，使得攻击者无法直接追踪到用户的真实位置和身份。代理服务器还可以对收发的数据进行过滤和审查，以确保数据的安全性。除了NAT和代理服务器，还有一种特殊的IP地址保护技术称为网络地址隐藏（NAN）。NAN是一种通过对IP地址自动进行动态分配和更改，使得攻击者无法追踪到真实的源IP地址的技术。具体实现时，NAN会在网络通信中应用一系列的技术手段，如IP地址伪造、路径躲避等，从而隐藏真实地址并提供匿名性。

4.5 信息加密处理

通过加密处理，可以将敏感的数据信息转化为不可读的形式，以防止未经授权的人读取和理解。信息加密处理采用不同的加密算法来实现。其中，对称加密算法是最常用的一种加密技术。对称加密算法使用相同的密钥对数据进行加密和解密。发送方将明文数据和密钥进行计算，生成密文后发送给接收方，接收方利用相同的密钥进行解密，恢复原始数据。常见的对称加密算法包括DES、AES等。另一种常用的加密技术是非对称加密算法，也称为公钥加密算法。非对称加密算法使用一对密钥，即公钥和私钥。发送方使用接收方的公钥对数据进行加密，接收方使用自己的私钥对加密后的数据进行解密。非对称加密算法主要用于密钥的安全交换和数字签名。常见的非对称加密算法包括RSA、ECC等。除了对称和非对称加密算法，还有哈希函数和消息认证码（MAC）等技术用于保证数据的完整性。哈希函数将任意长度的数据转换为固定长度的摘要，用于验证数据在传输中是否被篡改。而MAC则通过在数据上附加一个密钥生成的认证码，以验证数据的完整性和来源。常见的哈希函数包括MD5、SHA等，常见的MAC技术包括HMAC。为了增强数据的安全性，通常会采用混合加密方法。即使用对称加密算法对数据进行加密处理，然后再使用非对称加密算法对对称密钥进行加密，并发送给接收方。接收方收到加密的对称密钥后，使用自己的私钥对其进行解密，然后再使用对称密钥对收到的密文进行解密，从而获得原始的明文数据。

结语

随着网络攻击和数据泄露等安全威胁的不断增加，加强对数据的保护已成为一项紧迫的任务。通过合理配置和应用这些技术，能够有效保护网络通信中的数据信息安全，建立一个安全可靠的网络通信环境。随着技术的不断发展，网络安全威胁也在不断演变，因此，进一步的研究和创新仍然需要不断加强，以应对日益复杂的安全挑战。

参考文献

[1]刘贵强.网络通信中的数据信息安全保障技术分析[J].现代传输，2022，(05):49-52.

[2]康海连.网络通信中的数据信息安全保障技术[J].信息记录材料，2021，22(09):71-72.

[3]张高明,陈亚军.网络通信中的数据信息安全保障技术[J].电子元器件与信息技术,2020,4(10):20-21.

[4]宫月月，郭建勤，张胜平.网络通信中的数据信息安全保障技术研究[J].无线互联科技，2021，18（16）：3-4.

[5]窦怀振.网络通信中的数据信息安全保障技术研究[J].电脑知识与技术，2021，17（11）：43-44，53.