网络通信中的数据信息安全保障关键技术

王会鹏
支付宝（杭州）信息技术有限公司　浙江杭州　310001

摘　要：随着互联网技术的迅猛发展，网络通信已成为现代社会不可或缺的一部分，渗透到人们生活的每一个角落。但是，随着网络通信应用范围越来越广，数据信息安全的问题越来越突出。数据泄露，黑客攻击和网络病毒的威胁层出不穷，严重威胁个人隐私，企业利益甚至国家安全。所以，对网络通信数据信息安全保障关键技术进行探究具有重要意义。文章旨在通过对现阶段网络通信中数据信息安全的挑战进行深入的分析，探究行之有效的关键技术手段以促进网络通信安全，维护数据信息完整性与机密性。

关键词：网络通信；数据信息安全；保障技术

一、网络通信中数据信息安全的重要性

数据信息安全是网络通信的关键。在全球互联化与数字技术普及的背景下，通信数据数量越来越多，复杂程度越来越高，对数据安全构成威胁的手段渐趋复杂。网络通信含有个人隐私，企业机密以及政府信息等敏感信息，这些信息一旦外泄或者遭到恶意篡改都有可能给个人，企业以及国家带来严重经济损失以及信誉危机。

黑客及不法分子通常会利用网络通信存在的漏洞通过手段对信息数据进行盗取，截获或者破坏，从而造成信息泄露，身份盗窃以及数据篡改。尤其对于金融，医疗，电子商务等行业来说，数据完整性与保密性显得格外重要，确保信息传递时的安全性也就显得尤为重要。

为增强数据信息安全性，需要采用加密，身份认证以及网络监控技术手段。加密能够阻止未经许可的访问者对敏感数据进行诠释；身份认证可以保证数据接收者合法可靠；通过网络监控，我们可以实时地识别并避免可能的风险。组织要不断加强网络安全策略与教育、增强员工的认识、遵循最佳的安全实践。

不断健全的法律法规以及国际标准，也给信息安全带来了更加健全的保证。网络通信时代数据信息安全既要在技术上加强，又要多方合作，不断完善，筑牢网络安全防线才能应对威胁情况的变化。

二、网络通信中常见数据信息安全威胁

1. 外部攻击

黑客攻击通常是利用系统漏洞或者弱密码非法侵入，企图盗取，篡改或者摧毁目标数据。恶意软件，例如病毒、木马、勒索软件等，会通过伪装或捆绑在正常软件中，悄无声息地感染用户系统，从而窃取个人信息、破坏数据完整性或进行敲诈勒索。钓鱼网站采用模仿传统网站的策略，诱导用户输入如账号、密码、信用卡等敏感数据，这可能会导致用户的隐私被泄露和财产遭受损失。这些攻击手段在不断发展变化，日趋隐蔽与复杂，对用户数据安全造成巨大危险。所以用户一定要随时提高警惕并加强安全防护，比如使用强密码，经常更新软件，不要轻易点开不明链接来对付这些不断肆虐的外部威胁。

2. 内部泄露

内部泄露则是对数据信息安全的又一重大威胁，它主要与人为错误以及内部人员恶意行为有关。人为错误有可能来自于员工疏忽大意或者缺乏技能，比如对敏感数据的处理出现了误操作和误发送等问题，或者是把数据保存到了不安全地方，这就会造成数据泄露或者是非法访问。此外，内部人员恶意也是不容忽视的危险。一些员工会因为不满意和贪念等因素而有意透露企业或者顾客敏感信息。这一行为不但会带来巨大经济损失，而且会给组织声誉带来长期损失。为防范上述风险，机构要定期开展数据安全培训与意识提升、强化内部监管机制、执行严格访问控制与数据加密措施等。同时建立一个完整的审计与日志记录系统来及时发现并回溯任何疑似数据访问与泄露事件。通过上述举措，各组织能够更加有效地对自身关键数据资产进行保护并减少内部泄露风险。在这个以数据为驱动的年代里，保障数据信息安全非常重要，防止内部泄露是实现该目的的重点内容。

3. 网络通信协议的安全隐患

网络通信协议在其设计阶段可能会存在一些未被充

分考虑的安全漏洞，这些漏洞有可能被黑客所利用，从而给网络通信带来潜在的威胁。比如有些协议可能会对数据加密措施不到位，从而使传输的数据易于拦截、解密等。另外，某些协议可能未执行有效的身份验证机制致使攻击者能够伪造自己的身份，然后实施中间人攻击或者会话劫持等行为。也有的协议对不正常或者不正确的情况会出现安全问题，比如没有不正确的重试机制或者不正确的处理方式等，会被攻击者用来实现恶意代码或者触发服务拒绝攻击。针对上述问题，必须对网络通信协议进行不断地更新与完善，并强化数据加密与身份验证机制以保证其机密性，完整性与真实性。与此同时，还必须建立一套完整的错误处理与异常管理机制来避免攻击者钻这些空子。

三、数据信息安全保障关键技术探究

1.加密技术

加密技术是将数据经过变换或者处理后，使得数据在传输以及存储的过程当中不容易被未经授权的一方所获取或者解释。对称加密算法与非对称加密算法都属于常见加密技术。对称加密时，发送方与接收方用同一密钥加密解密数据以达到安全传递信息的目的，如DES，AES算法等；以及非对称加密是利用公钥与私钥对数据的加密与解密，其中公钥是加密的，私钥是解密的，如RSA算法等。除加密技术外，认证技术在数据信息安全保障中占据着至关重要的地位，采用数字证书与双因素认证相结合的方式来保证通信双方身份的真实性。在网络通讯领域，加密和认证两种技术互为补充，它们共同形成了一个安全的数据传输路径，有效地减少了数据外泄和网络攻击的可能性。在数字化信息时代的今天，加密技术应用已成为确保网络通信安全必不可少的重要工具，对建设安全、可靠的网络通信环境具有强大的支持作用。

2.认证技术

认证技术对网络通信起着关键作用，它保证了通信双方身份的真实性以及数据传输完整性。其中数字证书作为常用的认证技术之一，它利用证书颁发机构来认证用户身份信息的数字签名，以保证信息发送方的真实地位。此外，双因素认证技术还综合考虑很多因素来认证用户，其中常用的有密码，生物识别信息或者硬件令牌。该技术增强了用户身份验证安全性并阻止非授权接入。认证技术和加密技术共同作用，构建了一个安全而可靠的网络通信环境，确保了数据信息能够安全传输。采用数字证书与双因素认证相结合的技术手段对网络通信数据信息进行防护，有效防止身份伪造与数据篡改带来的安全威胁。在如今信息化社会中，认证的运用不但增强了网络通信安全性，而且给用户带来更方便、更可靠的数字服务体验。

3.访问控制技术

访问控制技术对于网络通信起着至关重要的作用，它用来管理控制用户访问系统资源权限、保障信息安全、数据保密性等。访问控制技术有访问控制列表，角色基础访问控制等。访问控制列表以策略规则作为访问控制的机制，它通过定义特定用户或者用户组许可或者拒绝接受资源访问的权限来达到细粒度的控制目的。并且角色基础访问控制是建立在对角色进行授权管理的基础上，赋予用户具体的角色及对应的权限，简化了权限管理并增强了系统的安全性与可管理性。该技术模式把权限授予人物，使用者通过该人物来获取对应权限，从而有效地减少权限管理复杂性。通过访问控制技术的合理分配，能够限制未授权访问，降低潜在的安全风险，从而使系统不受恶意攻击。访问控制技术有助于组织构建完善的信息安全保障体系并有效地保护敏感数据及重要资源免受未经许可访问。在现今网络环境下，由于数据规模越来越大，信息安全威胁也越来越大，访问控制技术发挥着越来越重要的作用，它已经成为保障网络通信安全，给用户及组织带来可靠信息安全保障的一个重要环节。

四、数据信息安全保障关键技术的具体应用

1.虚拟专用网络（VPN）技术

虚拟专用网络（VPN）技术是一种通过公共网络（如Internet）在私人网络间建立安全连接的技术手段。它采用隧道技术在公共网络中设置了一条特殊的虚拟信道，从而实现了该信道上的数据安全传输。VPN技术以安全性与隐私保护能力为核心。

VPN一般使用加密算法对数据私密性进行保护，例如AES，RSA加密协议保证数据不会在传输时被盗用和篡改。VPN利用隧道技术，例如PPTP、L2TP、IPSec等隧道协议，在公共网络中建立了一个安全的虚拟专用通道，这样数据就可以在该通道中传输，而不会受到外界的窥视或干扰。

VPN技术具有远程办公，跨地域接入，公共Wi-Fi安全防护，绕开地域限制等多种应用场景。通过VPN技术使用户能够随时随地安全的访问企业内部网络资源并进行远程办公；还可在企业不同办事处、分支机构间建立安全联系，共享数据、信息；当公共场所采用免费

Wi-Fi后，VPN能够对用户数据流量进行加密，避免黑客盗用个人信息；另外用户也可使用VPN来绕开地域限制进入具体站点及服务。

总体来看，VPN技术给用户在公共网络中建立安全连接，确保数据传输安全性以及用户隐私等方面提供了有效方法。

2.安全套接层（SSL）/传输层安全（TLS）协议

在网络通信领域，安全套接层（SSL）与传输层安全（TLS）的协议被视为确保数据和信息安全的核心技术。SSL，也被称为安全套接层协议，是Netscape公司在1994年推出的一种基于WEB应用的安全协议。而TLS作为SSL的后续版本，为用户提供了更加安全的通讯手段。

SSL/TLS协议在应用层与传输层间主要是对TCP/IP连接进行数据加密，服务器认证，消息完整性和可选择客户机认证等。这两个协议通过使用加密算法，如AES、RSA等，对在应用程序协议（如HTTP、FTP等）和TCP/IP协议之间传输的数据进行加密。这样的加密方式不仅确保了数据的保密性，还维护了数据的完整性，因为任何对正在传输的数据进行的篡改都可以通过消息认证码（MAC）来检测。

SSL/TLS协议的重要环节之一就是握手协议使服务器与客户机之间可以互相验证、协商加密与MAC算法、保密密钥等。这一流程包括了多个消息交换环节，涵盖了客户端与服务器间的hello消息交流、密钥的互换以及证书的验证等环节。经过这一系列的措施，双方成功地构建了一个安全的通信连接，从而确保了后续通讯活动的安全性。

SSL/TLS协议在Web浏览器与服务器间的各种通信方式，如电子邮件、实时通讯以及虚拟专用网络（VPN）中都有广泛的应用，其主要目的是确保数据传输的安全性。伴随着科技的进步，TLS已逐步替代SSL成为维护网络通信安全的主要协议。它的最新版TLS 1.3无论是安全性，性能还是兼容性均得到显著提高，给用户带来更高一级数据安全保障。

3.网络安全策略的制定与实施

在网络信息安全保障中，网络安全策略制定和执行处于核心地位。战略的制定需要考虑网络架构，业务需求和风险承受能力等方面的参数，并确定安全目标，原则和措施。其中包括识别受保护数据资产例如客户信息和交易数据之类敏感信息；确定潜在的威胁例如黑客攻击和数据泄露；对这些威胁所可能造成的危险进行评估并采取相应的预防措施。在实现阶段需要将安全策略细化到具体操作规程中，主要包括建立访问控制列表，防火墙配置规则和入侵检测系统敏感性调整。同时保证所有网络设备及系统满足安全策略要求如：安全加固服务器、约束不必要端口及服务、补丁及时更新。另外，经常性的安全培训与演练在策略实施过程中具有重要意义，能够促进职工安全意识与应急响应能力的提高。通过建立监控和审计机制，例如日志分析和异常检测等，可以确保安全策略的持续有效性，并能够及时调整策略以应对新出现的安全威胁。

结束语

在网络通信技术快速发展的背景下，给人们日常生活与工作带来巨大便利，但也引发了操作系统漏洞，网络信息盗窃以及黑客攻击等系列安全风险。这些威胁很容易让敏感信息落入不法分子手中，从而导致不可预知的危害。针对上述风险，提出了建设综合防火墙防护系统、采取高效网络数据加密措施以及身份验证技术等措施。另外，强化IP地址保护及网络安全行业监管是保障网络传输环境的安全、和谐及稳定，进而切实保障个人及企业数据安全的关键环节。

参考文献

[1]杨志贞.网络通信中的数据信息安全保障技术研究[J].电子测试，2021（04）：20.

[2]邵鲁科.计算机网络通信安全中数据加密技术的应用[J].数字技术与应用，2022（01）：25.

[3]章志勇，詹伟.网络通信中的数据信息安全保障技术分析[J].电子世界，2020（12）：30.

[4]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（04）：20.