计算机网络安全技术在电子商务中的应用

高俊阁

摘　要：随着电子商务的迅猛发展，计算机网络安全技术的应用变得愈加重要。电子商务平台在处理海量用户数据、进行在线交易的过程中，面临着各种安全威胁，包括数据泄露、网络攻击和身份盗用等。有效的计算机网络安全技术能够保护用户信息，维护交易安全，从而提升电子商务的整体可信度和运营效率。本文将探讨计算机网络安全技术在电子商务中的应用，分析这些技术如何保障电子商务平台的安全性。

关键词：计算机网络；安全技术；电子商务；应用

前言

在信息技术飞速发展的背景下，电子商务已经成为现代商业的重要组成部分。其发展不仅推动了经济增长，也改变了传统商业模式。随着网络攻击手段的不断演化，保护电子商务平台的安全性变得尤为关键。计算机网络安全技术作为保障电子商务安全的重要工具，发挥着不可或缺的作用。数据加密、身份认证、入侵检测系统等技术手段能够有效防范各种网络安全威胁，为用户提供安全可靠的交易环境。

1　应用在电子商务中的计算机网络安全技术

1.1 入侵检测技术

随着电子商务平台对数据和交易的依赖增加，网络攻击和入侵事件的风险也随之上升。入侵检测系统（IDS）能够实时监控网络流量和系统活动，识别潜在的安全威胁。通过分析异常行为和模式，这些系统可以检测到未经授权的访问尝试、恶意软件活动及其他可疑行为，从而及时发出警报并采取措施防止损害。这种技术通常包括基于签名的检测和基于行为的检测两种方法。基于签名的检测依靠已知的攻击特征进行识别，而基于行为的检测则通过分析正常和异常行为模式来发现潜在威胁。这种多层次的检测能力能够有效应对各种网络安全威胁，保护电子商务平台的完整性和用户数据的安全。

1.2 数据加密技术

数据加密技术通过将敏感数据转换为只有授权方能够解密的密文，防止数据在传输或存储过程中被窃取或篡改。数据加密不仅确保了用户的个人信息，如信用卡号码和登录凭证，得到有效保护，还增强了交易过程的安全性。在实际应用中，电子商务平台采用了多种加密算法，例如对称加密和非对称加密，以适应不同的安全需求。对称加密技术在数据传输中速度较快，适用于大规模数据处理，而非对称加密技术则用于加密密钥和验证身份，提供更高的安全保障。结合这两种加密方式，电子商务平台能够在保护用户数据的同时，确保交易的完整性和机密性。

1.3 身份认证技术

身份认证技术通过验证用户的身份，确保只有合法用户能够访问系统或进行交易。这项技术通常结合多种验证手段来提高安全性，例如密码、短信验证码、指纹识别或人脸识别等。通过这些多因素认证方法，系统能够显著减少非法访问和账户劫持的风险。在电子商务交易中，身份认证技术不仅保护用户的个人信息免受未经授权的访问，还能够防范各种网络攻击，如钓鱼攻击和伪造身份等。系统通过实时验证用户身份，及时发现并阻止异常登录尝试，从而维护了交易的安全性和平台的稳定性。

2　电子商务中的计算机网络安全问题

2.1 蠕虫病毒攻击

在电子商务中，蠕虫病毒攻击是一种常见且具有高度危害性的网络安全问题。这类病毒以自我复制和传播为特征，可以迅速感染计算机系统和网络，从而导致大量敏感数据的泄露或丢失。蠕虫通过漏洞进入系统后，会在不需要用户交互的情况下自动扩散，迅速占领连接到同一网络的其他设备。电子商务平台尤其容易受到蠕

作者简介：高俊阁（1988.10——），男，汉族，天津武清人，本科学历，中级工程师，主要研究方向为计算机管理、程序编写、IT运维等。

虫病毒的攻击，因为它们通常处理大量敏感信息，包括用户的个人数据和金融信息。一旦蠕虫感染了电商网站的服务器，可能会导致用户信息的泄露、账户被盗用，甚至交易记录的篡改。

2.2 数据泄露攻击

数据泄露攻击通常通过非法手段获取、公开或滥用敏感信息，包括用户的个人资料、支付信息和交易记录。攻击者可能利用系统漏洞、网络钓鱼或社会工程学手段侵入数据库或系统，从而窃取大量的用户数据。一旦数据泄露发生，企业不仅面临用户隐私的侵犯，还可能受到法律和合规风险的影响。泄露的敏感信息可能包括信用卡号码、身份证信息等，攻击者利用这些数据进行身份盗窃、金融诈骗等犯罪活动。这不仅对用户造成了直接的经济损失，也严重影响了企业的声誉和用户信任。

3 计算机网络安全技术在电子商务中的应用策略

3.1 小型电商网络设计

小型电商由于资源有限，往往成为网络攻击的目标，因此在网络架构的设计上需要格外谨慎。在网络拓扑结构上，小型电商应采用分层结构，将内部网络与外部网络隔离，通过防火墙和入侵检测系统等安全设备保护关键资产。网络的划分可以通过虚拟局域网（VLAN）实现，将不同功能区分开，以限制潜在的攻击路径。这种分层策略不仅减少了攻击面，也提高了网络的整体安全性[1]。在数据传输过程中，采用加密技术确保信息的安全传输非常重要。小型电商可以使用虚拟专用网络（VPN）在不同节点之间建立安全通道，防止敏感数据在传输中被截获或篡改。小型电商网络的设计还需兼顾扩展性，以应对未来业务增长。通过设计灵活的网络架构，企业可以在不影响安全性的前提下，平稳地扩展其网络基础设施。

3.2 防火墙安全策略

防火墙作为网络的第一道防线，负责监控和控制进出网络的数据流量，以防止未经授权的访问和潜在的网络攻击。通过精细的访问控制规则，防火墙能够有效限制外部威胁的进入，并在内部网络中创建不同的安全区域，以保护敏感信息。在防火墙策略的实施中，精确定义允许和拒绝的流量类型至关重要。管理员可以根据业务需求设置具体的访问控制列表（ACL），允许合法的数据流入和流出网络，阻止任何可疑或未授权的连接。通过这种策略，可以有效减少网络暴露面，降低攻击者通过漏洞进入系统的风险[2]。状态检测技术也是防火墙策略中的重要一环，它能够根据数据包的状态和上下文进行更智能的过滤，确保只有符合预期会话的数据包才能通过。这种技术提升了防火墙的判断力，使其不仅仅依赖于静态规则，而是能够动态调整，适应不断变化的网络环境。

3.3 防范攻击Web应用

Web应用是电子商务平台与用户交互的主要界面，也是攻击者最常瞄准的目标。为了有效防范攻击，必须采用多层次的安全措施来保护Web应用的安全性和完整性。输入验证是防范攻击的基础手段，通过严格的输入过滤和校验，可以防止SQL注入、跨站脚本（XSS）等常见攻击手段。通过对用户输入进行白名单过滤，限制输入内容的格式和范围，减少恶意代码注入的可能性。同时，利用安全编码实践，避免在代码中直接使用用户输入的数据，从源头上减少漏洞的出现。会话管理策略在防范攻击中起着重要作用[3]。通过使用安全的会话令牌，并在用户登录后自动生成唯一的会话ID，可以防止会话劫持和重放攻击。结合HTTPS加密传输，确保会话信息在网络传输中的安全性，进一步提高Web应用的防护能力。

结语

综上所述，计算机网络安全技术在电子商务中的应用对维护平台安全和用户信任至关重要。数据加密、身份认证和入侵检测系统等技术为电子商务提供了多层次的保护，防止了数据泄露和网络攻击。然而，随着网络攻击技术的不断进步，现有的安全措施也面临新的挑战。因此，电子商务平台需要不断更新和优化其安全策略，引入新技术和解决方案，以应对不断变化的威胁环境。

参考文献

[1] 邹聪.计算机网络安全标准化技术在电子商务中的应用[J].大众标准化，2023，(18)：148-150.

[2] 蔡晓阳.计算机网络安全技术在电子商务中的应用[J].电子技术，2023，52(08)：212-213.

[3] 戴香木.计算机网络安全技术在电子商务中的应用[J].中国管理信息化，2023，26(12)：191-193.