**重庆邮电大学《计算机网络》课程报告**

**2024-2025学年第 1 学期**

**题 目 网络安全技术的剖析与防范策略**

**姓 名 李恩熙**

**学 号 2022211780**

**专 业 计算机科学与技术**

**班 级 04012202**

**成 绩**

**2024年 12 月 10 日**

# 网络安全技术的剖析与防范策略

**摘 要：本论文聚焦于大数据时代计算机网络安全的现状与挑战，探讨了计算机网络安全技术在这一背景下的应用与发展。通过对相关文献的综合分析，阐述了大数据对计算机网络安全的多方面影响，详细解析了网络安全的关键技术，并提出了具有针对性的防范策略，旨在为提升计算机网络安全防护水平提供全面的理论依据与实践指导。**

**关键词：大数据；计算机网络安全；网络数据库；安全防范**

## 1 引言

随着信息技术的迅猛发展，大数据时代已然来临。海量数据的产生、存储、传输与分析在为各领域带来前所未有的机遇的同时，也使计算机网络安全面临着更为严峻的挑战。如何在充分利用大数据优势的基础上，确保计算机网络的安全性，已成为当今信息技术领域紧急需要解决解决的关键问题。

## 2 大数据对计算机网络安全的影响

### 2.1数据量急速增长带来的的挑战

大数据环境下，网络数据呈爆炸式增长，数据来源广泛、格式多样、结构复杂。这种海量且复杂的数据使得传统的网络安全防护手段难以应对，例如，在数据的存储与管理过程中，确保数据的完整性、保密性和可用性变得更加困难，因为需要处理和保护的数据量远远超出了以往的规模。

### 2.2 隐私泄露风险加剧

大数据分析往往涉及对大量个人信息的整合与挖掘，这在一定程度上增加了隐私泄露的风险。不法分子可能利用大数据技术的漏洞，获取用户的敏感信息，如个人身份信息、消费习惯、地理位置等，进而进行恶意利用，给用户带来严重的损失。

### 2.3 新型攻击手段的滋生

大数据的发展同时也催生了新型的网络攻击手段。攻击者可以利用大数据分析技术，更精准地定位目标，实施针对性更强的攻击，如高级持续性威胁（APT）等攻击。这些攻击往往具有隐蔽性强、潜伏期长、危害大的特点，传统的安全检测方法难以有效识别和防范。

## 3 计算机网络安全关键技术

### 3.1 网络数据库安全管理技术

#### 3.1.1 访问控制机制

网络数据库通过严格的访问控制机制，限制用户对数据的访问权限。比如，基于角色的访问控制（RBAC）模型，根据用户在组织中的角色分配相应的访问权限，确保只有授权用户能够访问特定的数据资源，从而有效防止非法用户的入侵和数据泄露。

同时，多因素身份验证技术也被广泛应用，如结合密码、指纹识别、短信验证码等多种方式，进一步增强用户身份认证的安全性，降低因账号被盗用而导致的数据安全风险。

#### 3.1.2数据加密技术

对网络数据库中的敏感数据进行加密存储是保障数据安全的重要措施。采用对称加密和非对称加密相结合的方式，给数据在存储和传输过程中的保密性提供双重保障。例如，在数据存储时，使用对称加密算法对数据进行快速加密，而在密钥管理和用户身份认证等环节，则利用非对称加密算法的特性，确保密钥的安全性和数据的完整性。

### 3.2 基于大数据的安全分析技术

#### 3.2.1 异常检测技术

利用大数据分析技术对网络流量和系统行为进行实时监测和分析，通过建立正常行为模型，可以做到及时发现异常行为。采用机器学习算法对网络数据进行训练，识别出与正常流量模式不同的异常流量，如大规模的数据传输、异常的端口扫描等，从而提前预警潜在的安全威胁。

关联分析技术也在异常检测中发挥着重要作用，通过对不同数据源和事件之间的关联关系进行分析，能够更全面地发现隐藏在复杂数据背后的安全隐患，提高安全检测的准确性和效率。

#### 3.2.2 威胁情报技术

威胁情报技术通过收集、整合和分析来自多个渠道的安全信息，如网络安全厂商的威胁情报库、开源情报等，为企业提供及时、准确的安全威胁预警。当出现新型的网络攻击手段或恶意软件爆发时，威胁情报系统能够快速将相关信息推送给企业，使其提前采取防范措施，降低安全风险。

## 4 计算机网络安全防范策略

### 4.1 强化安全意识与培训

#### 4.1.1 用户教育

对普通网络用户进行安全意识教育，使其了解网络安全的重要性以及常见的安全风险，比如说避免在不安全的公共网络环境中进行敏感信息操作、不随意点击可疑链接、定期更新密码等，从用户层面减少安全事故的发生。

#### 4.1.2 专业人员培训

针对网络安全专业人员，开展定期的培训课程，使其掌握最新的网络安全技术和防范策略，如大数据安全分析技术、新型加密算法等，提高其应对复杂安全挑战的能力，确保企业网络安全防护体系的有效运行。

### 4.2 完善安全管理制度

建立健全的数据安全管理制度，明确数据的收集、存储、使用、共享等各个环节的安全要求和操作流程。规定数据的分类标准和相应的安全防护级别，对不同级别的数据采取不同的加密、访问控制等措施，确保数据在全生命周期内的安全性。

制定完善的应急响应制度，当发生网络安全事件时，能够迅速启动应急预案，采取有效的措施进行应对，及时隔离受感染的系统、备份重要数据、开展调查取证等，最大限度地减少安全事件造成的损失，并快速恢复网络系统的正常运行。

### 4.3 加强技术创新与合作

企业和科研机构应加大对计算机网络安全技术研发的投入，鼓励创新，推动网络安全技术的不断发展。研发更高效的大数据安全分析算法、更安全的加密技术以及更智能的入侵检测系统等，以应对不断变化的网络安全威胁。

加强计算机网络安全行业内的合作与共享，建立安全信息共享平台，促进企业之间、企业与安全厂商之间的安全信息交流与合作。共享网络安全威胁情报、最佳实践经验等，共同提升整个行业的网络安全防护水平。

## 5 结论

在大数据背景下，计算机网络安全面临着前所未有的挑战，但同时也迎来了新的发展机遇。通过深入研究和应用网络数据库安全管理技术、基于安全分析技术等关键技术，并采取强化安全意识与培训、完善安全管理制度、加强技术创新与合作等防范策略，能够有效地提升计算机网络的安全防护水平，保障大数据时代网络信息系统的安全稳定运行，为个人、企业和社会的信息化发展奠定坚实的基础。

## 参考文献

1. 楚雅雯.基于大数据的计算机网络安全分析及防范 [J]. 计算机产品与流通，2020 (05):87.
2. 张玮.探析计算机网络数据库中的安全管理技术 [J]. 计算机产品与流通，2020 (05):40+78.
3. 蒋东晖.大数据背景下的计算机网络安全探析 [J]. 电脑编程技巧与维护，2020 (04):158-159+164.