# 数据加密技术在医院计算机网络通信安全中的应用

王 忱 宗晓祥*
宁夏医科大学总医院信息中心 宁夏 银川 750001

**摘 要：**随着医疗信息化的快速发展，医院计算机网络通信安全问题日益突出。本文旨在探讨数据加密技术在医院计算机网络通信安全中的应用，分析当前医院网络通信安全的现状与挑战，并提出相应的优化策略。通过文献综述和案例分析，本文详细阐述了数据加密技术在医院信息系统、计算机软件及局域网中的应用，并探讨了数据加密技术的选择与优化策略，以及与其他安全防护手段的结合。研究结果表明，数据加密技术在提升医院计算机网络通信安全方面具有重要作用，但仍需进一步优化和整合其他安全措施。

**关键词：**数据加密技术；医院计算机网络；通信安全；信息系统；局域网

## 引言

随着医疗信息化的深入发展，医院计算机网络通信安全问题日益成为关注的焦点。医疗数据的敏感性和重要性使得医院网络通信安全面临严峻挑战[1]。数据加密技术作为一种有效的安全防护手段，在医院网络通信安全中发挥着重要作用。

## 1 医院计算机网络通信安全现状与挑战

### 1.1 医院计算机网络通信安全现状分析

（1）医院计算机网络通信系统的构成及其特点

医院计算机网络通信系统主要由硬件基础设施（如服务器、交换机、路由器、工作站等）、网络操作系统、通信协议、数据库系统以及各类医疗应用软件构成。这些组件共同协作，确保医院内部各部门之间以及医院与外部机构之间的数据交换和信息共享。医院计算机网络通信系统的特点主要体现在以下几个方面：高度集成性：医院信息系统（HIS）、电子病历系统（EMR）、实验室信息系统（LIS）、影像归档与通信系统（PACS）等多个系统高度集成，数据交互频繁。实时性要求高：医疗过程中需要实时获取患者信息，如生命体征、检查结果等，对网络的实时性有很高要求。数据敏感性：医院网络中存储和传输的数据包含大量个人隐私和医疗敏感信息，需要严格保护。用户多样性：包括医生、护士、技术人员、管理人员以及患者等不同角色的用户，对系统的访问需求各异[2]。

（2）医院计算机网络通信面临的主要安全威胁

外部攻击：如黑客利用漏洞进行网络入侵，窃取或篡改数据，甚至植入恶意软件。内部威胁：医院内部员工可能因疏忽或恶意行为导致数据泄露，如未经授权访问敏感数据。病毒与恶意软件：通过电子邮件、外部存储设备或网络传播，对系统造成损害。网络钓鱼与社会工程学攻击：诱导用户点击恶意链接或下载恶意附件，从而获取敏感信息。物理安全威胁：如设备被盗、未经授权的物理访问等。

### 1.2 医院计算机网络通信安全挑战

（1）医院计算机网络通信安全面临的挑战

黑客攻击日益复杂：黑客利用高级持续性威胁（APT）、零日漏洞等复杂手段进行攻击，难以防范。内部人员非法访问：内部员工可能利用职权或技术手段非法访问、修改或删除敏感数据，且难以追踪。数据泄露风险高：医疗数据的敏感性使得一旦泄露，将对患者隐私、医院声誉乃至法律责任产生严重影响[3]。合规性要求严格：医疗行业面临严格的隐私保护和数据安全法规，如HIPAA（美国健康保险流通与责任法案）等，不合规将面临重罚。

（2）数据加密技术在应对这些挑战中的关键作用

确保数据保密性：通过加密敏感数据，即使数据在传输过程中被截获，也无法被未经授权的人员解读。增强数据完整性：加密技术可以附带数据完整性校验机制，确保数据在传输过程中未被篡改。减少内部威胁：即使内部员工试图访问加密数据，也无法直接读取，从而降低了内部泄露的风险。符合合规要求：数据加密是许多国家和地区隐私保护和数据安全法规的明确要求，有助于医院满足合规要求。

## 2 数据加密技术在医院计算机网络通信安全中的应用

**第一作者：**王忱，1972.02.06，男，学历：大专，职称：初级，研究方向：计算机

**第二作者：**宗晓祥，1988年7月，男，研究生，高级工程师，研究方向：医疗信息化

2.1 数据加密技术在医院信息系统中的应用

（1）作用及实现方式

数据加密技术在医院信息系统中的主要作用是保护敏感数据的安全性，防止未经授权的访问和数据泄露。医院信息系统中存储了大量的患者病历、诊断结果、治疗方案等敏感信息，这些数据的泄露不仅会对患者隐私造成严重侵害，还可能导致医疗事故和法律纠纷。因此，采用数据加密技术对这些敏感数据进行保护显得尤为重要。常见的实现方式包括对称加密和非对称加密[4]。对称加密使用相同的密钥进行加密和解密，适用于大量数据的快速处理，如AES（高级加密标准）算法。非对称加密则使用公钥和私钥，适用于数据传输过程中的安全验证，如RSA算法。对称加密和非对称加密的结合使用，可以在保证数据处理效率的同时，确保数据传输的安全性。

（2）应用案例

某大型医院采用AES（高级加密标准）对称加密算法对患者病历数据进行加密存储。AES算法以其高效性和安全性著称，能够对大量数据进行快速加密和解密，确保患者病历数据在存储过程中的安全性。在数据传输过程中，医院使用RSA非对称加密算法对数据进行加密，确保数据在传输过程中的安全性。RSA算法通过公钥和私钥的配对使用，能够有效防止数据在传输过程中被截获和篡改。通过这种方式，医院成功防止了多次外部攻击，保障了患者隐私。例如，在一次针对医院信息系统的网络攻击中，攻击者试图通过网络窃取患者病历数据，但由于数据已经通过AES和RSA算法进行了双重加密，攻击者无法解密数据，最终未能得逞。这一案例充分证明了数据加密技术在保护医院信息系统安全中的重要作用[5]。

2.2 数据加密技术在医院计算机软件中的应用

（1）具体应用

在医院计算机软件中，数据加密技术主要应用于加密存储、访问控制与权限管理。加密存储确保敏感数据在硬盘上以加密形式保存，即使物理设备被盗，数据也无法被轻易读取。访问控制与权限管理则通过加密技术确保只有授权用户才能访问特定数据，从而防止内部人员滥用数据。例如，在医生工作站中，患者的病历数据通常以加密形式存储在硬盘上。即使工作站的硬盘被盗，由于数据已经加密，窃贼也无法轻易读取和利用这些数据。医院通过权限管理系统，对不同角色的用户设置不同的访问权限。例如，只有主治医生才能访问特定患者的完整病历数据，而其他医护人员只能访问部分数据。这种权限管理机制通过加密技术实现，确保了数据访问的安全性和可控性。

（2）效果分析

通过实施数据加密技术，医院计算机软件的安全性得到了显著提升。某医院采用加密存储技术对医生工作站中的患者数据进行保护，同时通过权限管理确保只有特定医生才能访问特定患者的病历数据。这种措施有效防止了内部人员滥用数据，提升了系统的整体安全性。例如，在一次内部审计中，医院发现某位医生试图访问与其无关的患者病历数据。由于权限管理系统通过加密技术对数据访问进行了严格控制，该医生的非法访问请求被系统自动拒绝，从而避免了潜在的数据泄露风险[6]。这一案例表明，数据加密技术不仅能够保护数据的安全性，还能够有效防止内部人员滥用数据，提升医院信息系统的整体安全性。

2.3 数据加密技术在医院局域网中的应用

（1）实现方式及作用

在医院局域网中，数据加密技术主要用于保护数据传输的安全性。医院局域网是医院内部信息系统的重要组成部分，承载着大量的敏感数据传输任务。为了确保这些数据在传输过程中的安全性，医院通常采用VPN（虚拟专用网络）和SSL/TLS协议等加密技术。VPN通过加密技术在公共网络上创建安全的通信通道，确保数据在传输过程中不被窃取或篡改。例如，当医生在医院外通过互联网访问医院信息系统时，VPN可以为其创建一个安全的加密通道，确保数据在传输过程中的安全性[7]。SSL/TLS协议则确保数据在客户端和服务器之间的安全传输，广泛应用于医院信息系统的Web访问和数据传输过程中。

（2）应用案例

某医院在局域网中部署了SSL/TLS协议，确保医生在远程访问医院信息系统时的数据传输安全。通过这种方式，医院成功防止了多次中间人攻击，保障了数据传输的完整性和机密性。例如，在一次针对医院局域网的中间人攻击中，攻击者试图通过伪造的网络节点截获医生与医院信息系统之间的数据传输。由于医院已经部署了SSL/TLS协议，数据在传输过程中始终处于加密状态，攻击者无法解密数据，最终未能得逞。这一案例充分证明了SSL/TLS协议在保护医院局域网数据传输安全中的重要作用。

## 3 数据加密技术在医院计算机网络通信安全中的优化策略

3.1 数据加密技术的选择与优化

（1）选择合适的加密算法

在医院网络通信中，选择合适的加密算法是确保数据安全的首要步骤。常见的加密算法包括对称加密算法（如AES、DES）和非对称加密算法（如RSA、ECC）。对称加密算法具有加密速度快的优点，适合用于大量数据的传输加密；而非对称加密算法则适合用于密钥交换和数字签名，确保数据的真实性和完整性。AES（高级加密标准）：AES是目前广泛应用的对称加密算法，具有高安全性和高效性，适合用于医院网络中的数据传输加密。RSA：RSA是一种非对称加密算法，常用于密钥交换和数字签名，确保数据在传输过程中的安全性。

（2）优化加密密钥管理

密钥管理是数据加密技术中的关键环节。在医院网络中，密钥的生成、分发、更新和销毁都需要严格的管理机制。优化密钥管理可以有效提升数据加密的安全性。密钥生成：采用安全的随机数生成器生成密钥，确保密钥的随机性和不可预测性。密钥分发：通过安全的密钥分发协议（如Diffie-Hellman密钥交换协议）确保密钥在传输过程中的安全性。密钥更新：定期更新密钥，避免密钥长时间使用导致的安全风险。密钥销毁：在密钥过期或不再使用时，及时销毁密钥，防止密钥泄露[8]。

（3）加密协议的优化

加密协议的选择和优化对于保障医院网络通信的安全性至关重要。常见的加密协议包括SSL/TLS、IPSec等。SSL/TLS协议：SSL/TLS协议广泛应用于Web通信中，能够提供数据加密、身份认证和数据完整性保护。在医院网络中，可以通过优化SSL/TLS协议的配置，如启用强加密套件、禁用不安全的加密算法，提升通信安全性。IPSec协议：IPSec协议主要用于VPN通信，能够提供端到端的数据加密和身份认证。在医院网络中，可以通过优化IPSec协议的配置，如选择合适的加密算法和认证方式，确保数据在传输过程中的安全性。

3.2 数据加密技术与其他安全防护手段的结合

（1）与访问控制技术的结合

访问控制技术是保障医院网络安全的另一重要手段。通过将数据加密技术与访问控制技术结合，可以有效防止未经授权的访问和数据泄露。身份认证：在数据加密的基础上，采用多因素身份认证（如密码、指纹、智能卡等）确保只有合法用户才能访问敏感数据。权限管理：根据用户的角色和职责，设置不同的访问权限，确保数据只能被授权人员访问。

（2）与防火墙技术的结合

防火墙技术是医院网络的第一道防线，能够有效阻止外部攻击和恶意流量。通过将数据加密技术与防火墙技术结合，可以进一步提升网络通信的安全性。流量过滤：防火墙可以对进出医院网络的流量进行过滤，阻止恶意流量和攻击行为。加密通信：在防火墙内部，采用加密技术对敏感数据进行加密传输，确保数据在传输过程中的安全性。

（3）与入侵检测系统的结合

入侵检测系统（IDS）能够实时监控网络流量，检测并阻止潜在的攻击行为。通过将数据加密技术与入侵检测系统结合，可以有效提升医院网络的安全性。实时监控：IDS能够实时监控网络流量，检测异常行为和攻击行为。加密保护：在IDS检测到异常行为时，及时采取措施，如中断通信、加密数据等，确保数据的安全性。

**结论**

本文通过文献综述和案例分析，详细探讨了数据加密技术在医院计算机网络通信安全中的应用。研究结果表明，数据加密技术在提升医院网络通信安全方面具有重要作用，但仍需进一步优化和整合其他安全措施。未来研究可进一步探讨数据加密技术在医院网络通信安全中的应用效果，并提出更加有效的优化策略。

**参考文献**

[1]金蒙.计算机网络通信中的安全威胁与计算机防御策略探析[J].信息与电脑(理论版),2024,36(17):47-49.

[2]莫海辉.局域网环境背景下的计算机网络安全技术应用策略[J].信息记录材料,2023,24(11):51-53.

[3]吴国辉.多方安全计算在通信网络中的隐私保护与数据安全[J].现代传输,2023,(04):51-54.

[4]余松.基于数据加密技术的计算机网络通信安全研究[J].数字通信世界,2023,(07):25-27.

[5]李波,王健光.计算机网络信息安全中数据加密技术的应用研究[J].科技资讯,2023,21(11):10-13.

[6]陆敏.5G通信时代计算机网络信息安全问题浅析[J].中国新通信,2023,25(10):1-3+86.

[7]张晓华,孟庆东,王铎钦.基于无监督神经网络的局域网安全态势自动化评估方法[J].微型电脑应用,2023,39(03):104-107+115.

[8]于光许.信息化背景下计算机通信网络信息安全防护策略[J].信息与电脑(理论版),2023,35(04):239-241.