智能医院信息系统中的患者数据安全加密方法

魏忠琴[1] 陈丽阳[2]
WEI Zhongqin CHEN Liyang

摘 要 智能医院信息系统用户众多，权限各异，难以确保患者信息安全同时满足各用户查看需求，患者信息固定密钥加密过程效率低下、抵抗攻击能力不足。为此，提出一种智能医院信息系统中的患者数据安全加密方法。通过清洗与校验患者数据，统一数据格式。在系统初始化后，生成加密密钥。加密阶段，首先对患者数据明文进行 AES 加密，再对 AES 密钥进行 CP-ABE 加密，根据用户属性灵活设置访问权限。解密时，用户凭私钥恢复 AES 密钥，进而解密数据。实验证明，该方法加密解密时间不超过 2 s，处理效率极高 . 同时，加密数据抵抗攻击能力保持在 98% 以上，安全性较强。

关键词 智能医院信息系统；患者；数据；安全；加密

doi：10.3969/j.issn.1672-9528.2025.05.034

0 引言

智能医院信息系统作为现代医疗领域不可或缺的重要组成部分，其安全性与可靠性直接关系到患者的隐私保护和医疗服务的质量。在信息化时代，智能医院信息系统正面临着日益严峻的数据安全挑战。患者数据，包括病史、诊断记录、药物方案等敏感信息，一旦泄露或被篡改，将对患者造成极大的伤害[1]。因此，对患者数据进行加密存储和传输成为保障数据安全的必要手段。尽管传统的数据加密方法在一定程度上能够保护数据的安全，但又各自存在不足。例如，文献 [2] 提出了通过密钥的形式处理，对加密芯片、密钥和硬盘进行运算，同时存储数据至硬盘主分区，只有三者同时存在才可以进行数据读取和使用，以实现数据安全加密目标。然而，这种方法的运算过程复杂，加密效果不佳，且一旦硬件设备受损，数据恢复可能较为困难；文献 [3] 提出了一种方法，通过对内部网络职工客户端产生和存储的文档进行透明加密，实现安全加密。但透明加密速度较慢，不适用于大数据量的加密保护。

鉴于此，本文开展了智能医院信息系统中的患者数据安全加密方法的深入研究，提出更加完善的加密方案，以期为智慧医疗系统的发展提供有力的技术支持，旨在解决现有加密技术的不足，通过创新的加密算法和策略，提高数据加密的效率和安全性，确保患者数据在存储和传输过程中的安全。

同时，本研究还考虑到系统的可扩展性和兼容性，以适应不断变化的医疗环境和技术进步。通过这些努力，期望能够为智能医院信息系统提供一个更安全、高效和可靠的患者数据保护方案，从而推动智慧医疗系统的持续发展和进步。

1 智能医院信息系统中患者数据清洗与校验

在现代化的智能医院信息系统中，患者数据的收集与处理扮演着至关重要的角色。这些数据主要来源于各种医疗设备和系统，涵盖电子病历系统、影像系统、实验室信息系统等多个方面[4]。为确保这些数据的准确性和可靠性，以及后续数据安全加密的准确性和可靠性，必须执行一系列严格的数据清洗与校验流程。这些流程包括但不限于数据的完整性检查、一致性校验、准确性确认以及隐私保护措施的实施。通过这些步骤，可以确保患者信息的准确无误，同时保护患者隐私，避免数据泄露的风险。此外，智能医院信息系统还应具备高效的数据处理能力，以便快速响应医疗需求，提供及时的医疗服务。因此，数据收集与处理的效率和质量直接影响到整个医院的运营效率和患者满意度。

数据清洗的第一步是去除冗余和无效信息。这一步骤包括剔除重复的数据记录、空值、乱码以及明显错误的数据项，以确保数据集的纯净性[5]。接下来，需要对来自不同来源的数据进行格式统一化处理，例如将日期格式统一调整为 YYYY-MM-DD 的标准形式，数值格式则统一为小数点后保留两位，从而确保数据的一致性和可比性。

其次，对清洗后的数据进行完整性与一致性校验。完整性校验确保每个数据记录都包含必要的字段，无遗漏现象，这可以通过计算字段完整率来衡量：

1. 甘肃中医药大学第四附属医院 甘肃兰州 730060
2. 浙江中医药大学 浙江杭州 311402

$$P_w = \frac{M_r}{M} \times 100\% \quad (1)$$

式中：M_r 表示完整记录数，即包含所有必要字段的数据记录的数量；M 表示总记录数，即数据集中所有记录的总数。通过该公式，直观反映数据集的字段完整性情况。

一致性校验是一种重要的数据处理步骤，主要负责检查来自不同来源的数据是否一致，确保关键信息如姓名、年龄、性别等在各个系统是否一致，未出现矛盾或错误 [6]。

在完成一系列的数据清洗和校验流程之后，这些经过处理的数据将被反馈给智能医院信息系统，用于后续患者数据安全加密处理以及数据分析工作，确保医院信息系统能够更加高效和准确地处理患者信息。

2 患者数据安全加密密钥生成

智能医院信息系统中患者数据清洗与校验完成后，初始化智能医院信息系统，生成加密密钥。

系统初始化时，授权中心会接收一个隐含的安全参数 λ 作为输入，并据此输出系统公钥 PK 和系统主密钥 MK。首先，选择一个素数 p，既是双线性群 G，也是其对应的目标群 G_T 的阶 [7]。选定 G 的一个生成元 g，用于构建群内的所有元素。确立双线性映射 $e: G \times G \to G_T$，满足双线性性质，即对于群 G 中的任意元素 g_1 和 g_2，以及任意整数 a 和 b，公式表示为：

$$e\left(g^a, g^b\right) = e(g,g)^{ab} \ \forall a,b \in Z_p \quad (2)$$

随机选取两个与素数 p 互素的整数 α 和 β，将作为主密钥 MK 的一部分。定义一个哈希函数 $H: \{0,1\}^* \to G$，该函数能够将任意长度的二进制字符串映射到群 G 中的某个元素。这个哈希函数为群 G 提供了一个丰富的随机元素库。在此基础上，生成系统公钥与主密钥，表达公式分别为：

$$\mathrm{PK} = \left(g, e(g,g)^{\alpha}, \{H_i(\cdot)\}_{i\in[1,n]}, H_i(\cdot)\right) \quad (3)$$

$$\mathrm{MK} = (\alpha, \beta) \quad (4)$$

针对具有不同属性集合 $A = \{A_1, A_2, \cdots, A_n\}$ 的用户，在整数集 Z_p 中随机选择一个整数 r。计算私钥的主组件 $D = g^r$。对于属性集合 A 中的每个属性 A_i，计算对应的私钥组件：

$$D_i = H_i(r)^{\alpha} \quad (5)$$

用户的私钥 K 最终表达为：

$$K = \left(D, \{D_i\}_{i\in[1,n]}\right) \quad (6)$$

即主组件 D 和所有属性对应的私钥组件 D_i 的集合。

通过这一密钥生成过程，智能医院信息系统为后续的患者数据混合加密处理奠定了坚实的基础。

3 患者数据混合加密处理

密钥生成后，为确保患者数据的安全传输，结合医疗数据的特性，设计了如图 1 所示的患者数据混合加密处理方案。

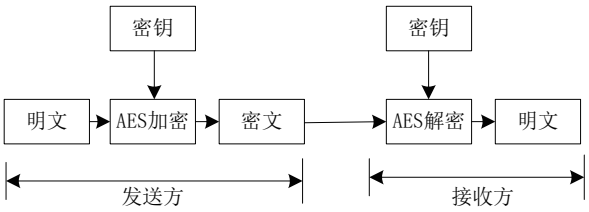


图 1 患者数据混合加密处理方案

此方案充分利用 AES 算法的高效加密性能和 CP-ABE（基于属性的加密）算法的细粒度访问控制特性，旨在为患者数据提供全方位的安全保障 [8]。

如图 1 所示，在加密阶段，首先对患者数据明文 M 进行 AES 加密处理。使用 AES 算法和上节生成的密钥 K，对患者数据明文 M 进行加密，得到第一次加密后的密文 M_1。加密公式表示为：

$$C_1 = \mathrm{AES}(K, M) \quad (7)$$

随后，使用 CP-ABE 算法对 AES 密钥 K 进行进一步加密，以确保密钥的安全传输 [9]。输入系统公钥 PK、预设的访问结构 A* 以及待加密的 AES 密钥 K，输出加密后的密文 CT。访问控制结构 A* 设定为 $(\boldsymbol{L}, \rho)$，其中 $\boldsymbol{L}$ 是一个 $1 \times n$ 的矩阵（1 代表用户属性数，n 代表 CP-ABE 访问策略中的属性数），ρ 是一个函数，用于将矩阵 $\boldsymbol{L}$ 的行与用户属性进行关联 [10]。选择一个随机向量 $\boldsymbol{s} = (s_1, s_2, \cdots, s_l) \in \mathbb{Z}_p^l$（$\mathbb{Z}_p$ 表示模 p 的整数集），用于分享加密元素。对于矩阵 $\boldsymbol{L}$ 的第 i 行 λ_i，计算公式为：

$$\lambda_i(s) = \sum_{j=1}^{n} s_{ij} \cdot s_j \ (\mathrm{mod}\ p) \quad (8)$$

最终得到密文组件，计算公式分别为：

$$C'' = g^{\beta s} \cdot H(K)^{\alpha s} \quad (9)$$

$$C_j = g^{\beta s j} \quad (10)$$

$$C_i'' = H_i(s)^{\alpha \rho(i)^{-1}} \quad (11)$$

式中：H 表示哈希函数；H_i 表示针对属性 A_i 的哈希函数；$\rho(i)$ 表示函数 ρ 将矩阵 $\boldsymbol{L}$ 的第 i 行与属性关联的映射值 [11]。

在解密阶段，需要输入具备用户属性集合 A' 的私钥 SK' 和密文 CT[12]。假设 A' 满足访问结构 A*，使用私钥 SK' 和密文 CT，通过线性秘密共享方案在多项式时间内恢复出 AES 密钥 K'。使用恢复出的 AES 密钥 K'，对第一次加密后的密文 C_1 进行解密，得到原始的患者数据明文 M，解密公式表示为：

$$M = \mathrm{AES}^{-1}(K', C_1) \quad (12)$$

综上所述，该患者数据混合加密处理方案通过将 AES 算法的高效加密性能与 CP-ABE 算法的细粒度访问控制特性相

结合，为智能医院信息系统中的患者数据提供了强有力的安全保障[13]。此方案不仅确保了数据的机密性，还实现了对数据的细粒度访问控制，从而有效防止了未经授权的访问和数据泄露。

4 实验分析

4.1 实验准备

实验聚焦于智能医院信息系统中的患者健康数据作为样本，涵盖四大类信息。如表 1 所示。

表 1 实验数据概览

序号	数据	描述
1	个人信息	包括患者的姓名、年龄、性别、联系方式等基本信息。
2	病史记录	包括患者的过往病史、手术记录等详细病史信息。
3	检查结果	包括患者的各项检查结果，每项检查结果都包含具体的数值和诊断意见。
4	诊断报告	包括医生对患者的诊断意见和治疗建议。

在本次进行的实验中，收集并使用了大约 1 000 条来自患者的详细数据记录。每一条数据记录都包含了表 1 所列出的多个关键字段，这些字段涵盖了患者的个人信息、病历记录、治疗方案以及随访结果等重要信息。每条数据记录的大小大约在 1 kB~10 kB 之间，这一范围的确定是基于数据记录的详尽程度以及其中包含信息的复杂性来决定的[14]。

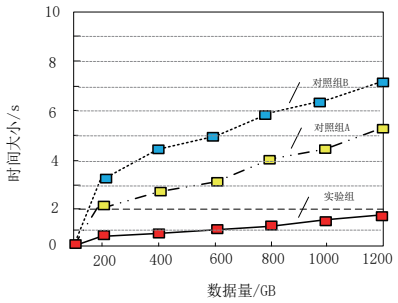
实验的环境是一个精心设计的模拟智能医院信息系统，能够高度仿真真实世界中的医疗数据处理和管理流程。该系统运行在一个配置了 Intel(R) Xeon(R) CPU（主频为 2.8 GHz）、拥有 8 GB RAM 的服务器之上。客户端方面，使用 Windows 10 操作系统的计算机。为保证网络通信的高效和稳定，实验环境还配备了路由器和交换机等高速网络设备，共同构成了一个能够支持快速数据传输和处理的网络架构[15]。

4.2 加密结果分析

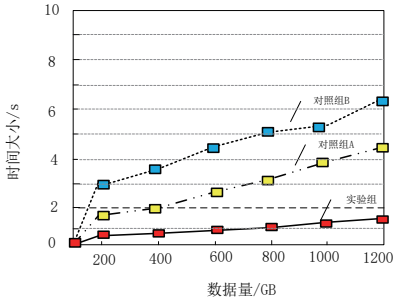
为确保实验的顺利进行，实验将在一个稳定的网络环境下开展，目的是排除网络波动可能对测试结果带来的潜在干扰，进而保证实验数据的精确度和可信度[16]。

在本次实验中，采用上文所提出的关于患者数据安全的加密方法作为实验组，与此同时选取文献 [2] 和文献 [3] 中所描述的两种传统的加密方法，分别作为对照组 A 和对照组 B。通过这样的设置，能够全面地比较和分析 3 种不同加密方法在加密效率以及抵御各种网络攻击能力方面的性能表现。

为确保加密和解密时间的精确度，实验中将对每一条患者数据执行多次加密和解密操作，并将计算所有操作的平均时间作为最终结果。患者数据安全加密效率的对比结果已直观呈现于图 2 中。



（a）加密时间



（b）解密时间

图 2 加密与解密时间比较

通过分析图 2 所展示的对比结果，可以清晰地观察到，实验组所采纳的患者数据安全加密技术在加密以及解密的效率方面，均明显超越了对照组 A 和对照组 B。具体来说，实验组所采用的方法在执行加密和解密操作时所消耗的时间，明显少于其他两组，其时间上限不超过 2 s。这一显著优势表明，在处理大规模患者数据时，实验组的方法展现出了更高的效率和处理速度。

基于上述发现，研究者们进一步深入研究了在不同患者数据安全加密量级（数据量范围从 200 GB 逐步增加至 1 200 GB，每次增加的量为 200 GB 的条件下），3 种不同的加密方法在抵御外部攻击方面的表现。通过对比分析，得到了如图 3 所示的结果，这些结果揭示了不同加密方法在面对不同数据量级时的安全性能差异。

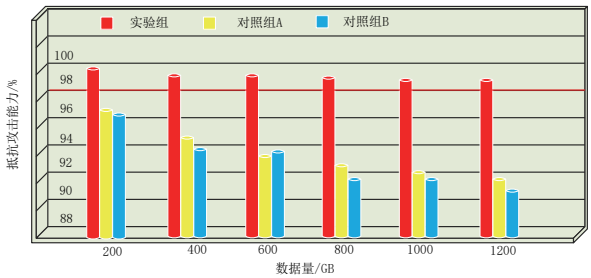


图 3 抵抗攻击能力对比结果

观察图 3 可以看到，随着患者数据安全加密数据量的持续增长，本文所提出的安全加密方法表现出了显著的优越性。其在抵抗各种攻击方面的能力始终稳定在 98% 以上的高水平，充分证明了该方法在面对各种潜在攻击时的卓越性能，

能够有效地确保智能医院信息系统中患者数据的安全性和机密性不受侵犯。此外，该方法所表现出的高抵抗攻击能力也意味着在数据传输的过程中，数据遭受攻击和篡改的可能性得到了显著降低，从而进一步提升了智能医院信息系统中隐私信息数据传输的可靠性和完整性[17]。

5 结语

随着医疗信息化进程的不断深入，智能医院信息系统在临床实践中的作用变得越来越重要。然而，患者数据的安全性问题始终是限制其进一步发展的主要障碍之一。为有效解决这一难题，本文深入探讨了智能医院信息系统中患者数据安全的加密技术，并取得了一系列具有突破性的成果。在本文中，提出了一套全面的数据加密方案，该方案包括了数据清洗与校验、密钥生成以及混合加密处理等多个关键环节。通过采用先进的加密算法和引入随机性高的密钥生成机制，显著提升了数据加密的强度[18]。此外，混合加密处理策略的运用，进一步加强了数据的抗破解能力。这套方案不仅能够有效增强患者数据的安全性，而且在保持高效运行的同时，能够抵御各种潜在的网络攻击威胁，具有深远的研究价值。

展望未来，本文将继续深化在智能医院信息系统患者数据安全领域的研究工作，致力于为患者数据的安全保护提供更加全面和高效的解决方案。尽管本文提出的加密方案已在智能医院信息系统中取得了一定的突破性成果，但随着技术的不断发展，新的网络攻击形式和数据安全挑战仍不断出现。因此，本文的研究工作并非终点，而是一个新的起点。在未来的研究中，将继续深入探讨更为高效、更加安全的数据加密技术，探索量子加密、同态加密等新兴技术在智能医院信息系统中的应用可能性。同时，随着医疗行业的信息化水平不断提高，患者数据的隐私保护也将成为越来越重要的议题。希望通过持续的技术创新，为智能医院信息系统提供更加全面、安全且高效的数据加密解决方案，从而为患者的隐私保护和医疗服务的高效性提供更加坚实的保障。

参考文献：

[1] 夏晓亮 , 秦智 , 万武南 , 等 . 基于区块链的医疗数据分类加密共享方案 [J]. 应用科学学报 , 2024, 42 (4): 613-628.

[2] 鲍婧 , 林炜峰 , 王学理 . 基于集成平台的互联网医院数据加密传输方案设计与实现 [J]. 中国数字医学 , 2024, 19 (7): 97-101.

[3] 张华贵 , 张俊萌 . 医院信息系统中的数据安全与隐私保护 [J]. 电脑知识与技术 , 2024, 20 (18): 67-69.

[4] 王新 , 冯英 , 杜炜 , 等 . 互联网传输中医院就诊数据安全加密方法研究 [J]. 自动化技术与应用 , 2024, 43 (6): 74-77.

[5] 孙煦 . 基于区块链技术的健康医疗数据隐私加密控制系统设计 [J]. 计算机测量与控制 , 2024, 32 (3): 188-194.

[6] 蒲亮 , 姚树智 , 敖继威 . 基于方差特征选择与 3DES 加密算法的医院信息数据安全防御系统设计 [J]. 计算机测量与控制 , 2024, 32 (5): 253-259.

[7] 高改梅 , 史旭 , 刘春霞 , 等 . 一种基于区块链的医疗数据隐私保护方法 [J]. 计算机应用研究 , 2024, 41 (5): 1538-1543.

[8] 郭庆 , 田有亮 . 支持受控共享的医疗数据隐私保护方案 [J]. 西安电子科技大学学报 , 2024, 51 (1): 165-177.

[9] 李小立 , 唐春霞 , 程玉柱 . 基于区块链的健康养老数据隐私保护系统设计 [J]. 长沙民政职业技术学院学报 , 2023, 30(2): 125-128.

[10] 任超 , 李雅瑜 . 数字经济时代数据隐私的反垄断保护：理论证成、适用困境及破解之道 [J]. 重庆邮电大学学报 (社会科学版),2023,35(4):65-75.

[11] 刘晶 , 朱家豪 , 袁闰萌，等 . 非独立同分布工业大数据下联邦动态加权学习方法 [J]. 计算机集成制造系统 , 2023, 29(5): 1602-1614.

[12] 苏晨 , 邹云峰 , 祝宇楠，等 . 一种基于差分隐私的电力客户数据隐私保护聚类方法 [J]. 电力需求侧管理 , 2023, 25(2): 101-106.

[13] 杨祖卿 . 数字市场中的数据隐私保护：维度拓展、实践困境及路径突破：基于反垄断法视角 [J]. 南方金融 , 2023(1): 65-77.

[14] 王利娥 , 王艺汇 , 李先贤 .POI 推荐中的多源数据融合和隐私保护方法 [J]. 广西师范大学学报 (自然科学版), 2023, 41(1): 87-101.

[15] 曹文继 , 宋彪 , 高海涛，等 . 大数据隐私保护过程中的博弈目标漂移现象及其控制 [J]. 内蒙古大学学报 (自然科学版), 2022, 53(5):522-529.

[16] 晏燕 , 丛一鸣 , MAHMOOD A, 等 . 基于深度学习的位置大数据统计发布与隐私保护方法 [J]. 通信学报 , 2022, 43(1): 203-216.

[17] 昌燕 , 林雨生 , 黄思维 , 等 . 面向工业互联网隐私数据分析的量子 K 近邻分类算法 [J]. 计算机研究与发展 , 2022, 59(5): 1082-1091.

[18] 陈子秋 , 冯瑞珏 , 郑扬富 , 等 . 非侵入式负荷监测系统数据隐私保护方法研究 [J]. 电子技术应用 ,2021,47(12):116-119.

【作者简介】

魏忠琴（1974—），女，甘肃白银人，硕士研究生，工程师，研究方向：软件设计。

陈丽阳（2004—），女，甘肃庆阳人，本科在读，研究方向：临床药学。

（收稿日期：2024-12-17 修回日期：2025-05-22）