DOI:10.20033/j.1003-7241.(2026)06-0149-07

基于深度强化学习的数字化医院病历数据加密研究

王诚斌, 王 辉

(上海市眼病防治中心 医务护理办公室, 上海 201103)

摘 要:为了提高电子病历(electronic medical record,EMR)共享调阅安全,应对隐私泄露、数据滥用风险,研究创新地基于深度强化学习(deep reinforcement learning,DRL)与深度学习完成了病历敏感信息的命名实体识别(named entity recognition,NER),然后采用高级加密标准(advanced encryption standard,AES)设计了病历数据加密模型。实验结果表明,基于深度强化学习的命名实体识别模型最高分类准确率可达 0.941、匹配准确率可达 0.901、F_1 值可达 0.876。在电子病历库中,该方法的标准化语义等级达 0.90,有利于加密算法的性能提升,基于深度强化学习的加密算法实现了最短密钥生成时间,最多耗时 559.93 ms;抵抗攻击的性能显著增加。研究设计的病历数据加密模型有助于保障患者的隐私权益和医疗安全,促进医疗资源的优化配置。

关键词:深度强化学习;DDPG 模型;电子病历;加密算法;深度学习;命名实体识别

中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1003-7241(2026)06-0149-07

Digital hospital medical record data encryption based on deep reinforcement learning

Wang Chengbin, Wang Hui

(Medical Nursing Office, Shanghai Eye Disease Prevention and Treatment Center, Shanghai 201103, China)

Abstract: To enhance the security of electronic medical record (EMR) sharing and retrieval, and address the risks of privacy leakage and data abuse, this study innovatively utilizes deep reinforcement learning (DRL) and deep learning to complete named entity recognition (NER) of sensitive medical record information. Subsequently, an encryption model for medical record data is designed using the advanced encryption standard (AES). Experimental results show that the DRL-based NER model achieves a maximum classification accuracy of 0.941, a matching accuracy of 0.901, and an F_1 score of 0.876. In the EMR database, the standardized semantic level of this method reaches 0.90, which is conducive to improving the performance of encryption algorithms. The DRL-based encryption algorithm achieves the shortest key generation time, with a maximum time consumption of 559.93 ms; its resistance to attacks significantly increases. The designed encryption model for medical record data helps to safeguard patients′ privacy rights and medical safety, and promotes the optimal allocation of medical resources.

Keywords: deep reinforcement learning; DDPG model; electronic medical records; encryption algorithm; deep learning; identity of named entity

医疗数据共享在推动医学研究、提高临床决策质量以及促进公共卫生发展等方面具有巨大的潜力。随着大数据、人工智能等技术的快速发展,医疗信息化水平不断提升,中国多地医院开始试行电子共享病历。电子共享病历提高了医疗服务的效率和质量,促进了医疗资源的优化配置,电子病历共享调阅已取得了显著成效[1-2]。电子病历涵盖了患者的基本信息、疾病诊断信息以及医嘱用药信息,患者的隐私保护、病历数据安全成为规范电子病历的关键环节。尽管国家相关部门已出台一系列法规文件为电子病历的共享调阅提供了法律保障,但电子病历在云存储环境下仍容易遭受恶意攻击、泄露以及不规范地滥用[3-4]。

针对医疗相关数据的隐私保护,国内外学者展开了广泛的分析。王玉珏[5]提出了一种混合加密系统用于保护医疗科研数据,该系统可实现数据资源的独立分配,解密平均错误 bit 数量明显降低。保护患者隐私是实现医疗数据共享的前提,Fugkeaw 等[6]集成了雾计算、基于属性的密文策略和区块链技术设计了一种安全物联网医疗数据传输和聚合方法,该方法在终端用户设备上加密和解密的处理成本较小。但电子病历非结构化数据,多为自由文本

收稿日期:2025-02-23;**录用日期**:2025-03-26

基金项目:上海市自然科学基金项目(22ZR1201200)

作者简介:王诚斌(1984—),男,中级工程师,研究方向:医疗大数据应用。

通信作者:王 辉(1989—),男,中级工程师,研究方向:医疗大数据分析。

引用本文:王诚斌, 王辉. 基于深度强化学习的数字化医院病历数据加密研究[J]. 自动化技术与应用, 2026,45(6):149-154, 168. (Wang Chengbin, Wang Hui. Digital hospital medical record data encryption based on deep reinforcement learning[J]. Techniques of Automation and Applications, 2026,45(6):149-154, 168.)

的半结构化形式,增加了数据处理难度并导致传统加密技术的适用性较差或性能欠佳。

为了提高加密技术面对非结构化数据的应对能力,该研究有望成为提高电子病历数据安全性和共享效率的重要途径。

1 医院病历数据加密研究

1.1 病历命名实体识别

NLP是一种自然语言处理技术,主要用于从文本中识别具有特定意义的实体。研究将其引入医疗领域,从电子病历中抽取出病症、体征、疾病、身体部位等关键信息。定义医疗实体集合由疾病、症状、用药、检查结果组成。数据预处理是NLP任务的关键,将自由文本转换成模型可理解和处理的形式[7]。研究将电子病历转换为带索引的词汇表,根据索引id转换文本数据。研究构建的NER模型由输入层、编码层和解码层,结构形式组成如图1所示。

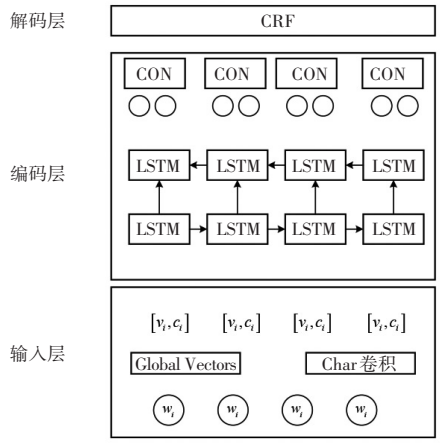


图1 NER模型结构组成

Fig. 1 Structure of the NER model

由图1可见,输入层、编码层和解码层分别由词向量模型、长短期记忆网络(long short-term memory,LSTM)的变形以及条件随机场(conditional random field,CRF)构成。输入层主要负责将文本序列 $s=\{w_1,w_2,\cdots,w_n\}$ 转化成对应的单词向量 $\boldsymbol{X}=\{x_1,x_2,\cdots,x_n\}$,其中 w_i 表示单词;单词向量 $\boldsymbol{x}_i=[\boldsymbol{v}_i,\boldsymbol{c}_i]\in\mathbb{R}^{d_w}$,$\boldsymbol{v}_i$ 表示预训练词向量、$\boldsymbol{c}_i$ 表示基于字符的词向量,d_w 表示向量维度。研究分别采用Global Vectors模型、Char卷积模型生成 v_i、c_i。此外,输入层使用标签嵌入捕捉标签 $L=\{l_1,l_2,\cdots,l_k\}$ 之间的依赖关系。

编码层包括双向LSTM(bidirectional long short-term memory,BiLSTM)、键值记忆网络(key-value memory networks,KV- MemNNs)和级联层。LSTM由遗忘门 f_t、输入门 i_t、输出门 O_t 组成,见式(1)。

$$\begin{cases} i_t=\sigma(W_i[y_{t-1},x_t]+b_i) \\ O_t=\sigma(W_o[y_{t-1},x_t]+b_o) \\ f_t=\sigma(W_f[y_{t-1},x_t]+b_f) \end{cases} \tag{1}$$

式中,σ 为激活函数;W、b 分别表示权重、偏置。LSTM隐藏层输出 y_t 计算见式(2)。$\boldsymbol{X}=\{x_1,x_2,\cdots,x_n\}$ 输入BiLSTM后,即可获得单词对应的隐藏状态向量。

$$y_t=O_t\tanh(S_t) \tag{2}$$

式中,S_t 表示LSTM内部状态。BiLSTM是LSTM的扩展版本,可同时处理序列数据中的前向和后向信息,由两个方向的网络组成,分别捕捉序列中的过去、未来上下文信息[8]。获得上下文表示向量后,标签嵌入向量 $\boldsymbol{l}_i$ 计算过程见式(3)。

$$\boldsymbol{l}_i=\sum_{j=1}^{k}p_{ij}e^{\mathrm{l}}(\boldsymbol{l}_j) \tag{3}$$

式中,p_{ij} 表示标签概率分布的第 j 个分量;e 表示标签嵌入向量查找表。KV- MemNNs通过键值对存储和检索信息,可支持复杂的推理任务。在NER模型中,KV-MemNNs利用上下文表示向量与 $\boldsymbol{l}_i$ 帮助命名实体预测,构成记忆槽中的向量对 $(\boldsymbol{k},\boldsymbol{v})$。KV-MemNNs主要由记忆模块、寻址模块和读取模块组成,记忆模块以 $(\boldsymbol{k},\boldsymbol{v})$ 的形式存储信息,寻址模块负责根据查询在记忆模块中查找相关的键,读取模块则根据找到的键读取对应的值作为输出或进一步推理地输入[9-10]。

级联层是将文档级别的上下文信息、标签嵌入信息与当前单词的上下文信息融合,以生成更精确的命名实体识别标签得分[11]。级联操作计算见式(4)。

$$\boldsymbol{g}_i=[\boldsymbol{h}_i;\boldsymbol{r}_i^{\mathrm{h}};\boldsymbol{r}_i^{\mathrm{l}}] \tag{4}$$

式中,$\boldsymbol{h}_i$ 表示单词的隐藏状态向量;$\boldsymbol{r}_i^{\mathrm{h}}$ 表示文档级上下文表示向量;$\boldsymbol{r}_i^{\mathrm{l}}$ 表示文档级标签嵌入向量。最后解码层使用CRF完成结果的序列标注,优化命名实体标签得分。标签得分计算见式(5)。

$$s(x,y,\theta)=\sum_{i=1}^{N}(\boldsymbol{T}_{y_{i-1}y_i}+E_{iy_i}) \tag{5}$$

式中,y_i 表示标签序列;iy_i 表示第 i 个单词的第 y_i 个标签序列的得分;$\boldsymbol{T}$ 表示转移分数矩阵;θ 表示参数。此外,研究采用DRL技术对实体标签进行修正,选用深度确定性策略梯度(deep deterministic policy gradient, DDPG)模型。DDPG是一种基于Actor-Critic框架的DRL算法,能够解决连续性控制问题的算法,DDPG网络模型结构如图2所示。

由图2可见,DDPG由Actor-online、Critic-online、Actor-target、Critic- target 4个神经网络组成。Actor-online负责生成一个确定性的动作,Critic-online负责评估动作的价值;同时双重神经网络模型,利用Actor-target、Critic-target评估和更新对应网络的参数。DDPG的经验缓存池则通过存储和回放经验数据,随机抽取批量数据进行训练,提升算法收敛性能。

DDPG首先初始化神经网络、经验缓存池以存储交互数据,并定义状态与动作。Critic网络利用Target网络计算目标值,并利用Online网络预测当前目标值,最后根据两者之间的均方误差损失来更新Online网络的参数。Actor网络利用Critic网络输出的目标值作为反馈,通过梯

度上升来更新 Actor 网络的参数,以使得输出的动作能够最大化目标值,更新过程见式(6)。

$$\nabla_\theta J(\theta)=\mathrm{E}_{s\sim p^\pi,a\sim\pi_\theta}[\nabla_\theta\log\pi_\theta(a\mid s)Q^\pi(s,a)] \tag{6}$$

式中,p^π 表示状态分布,π 为策略,θ 为对应参数;$Q^\pi(s,a)$ 表示当前状态 s 和动作 a 的价值。Critic-online 参数 θ^Q 更新过程见式(7)。

$$L_i(\theta^Q)=(y_i^{'}-Q(s_i,a_i\mid\theta^Q))^2 \tag{7}$$

式中,$y_i^{'}$ 表示时序差分目标。

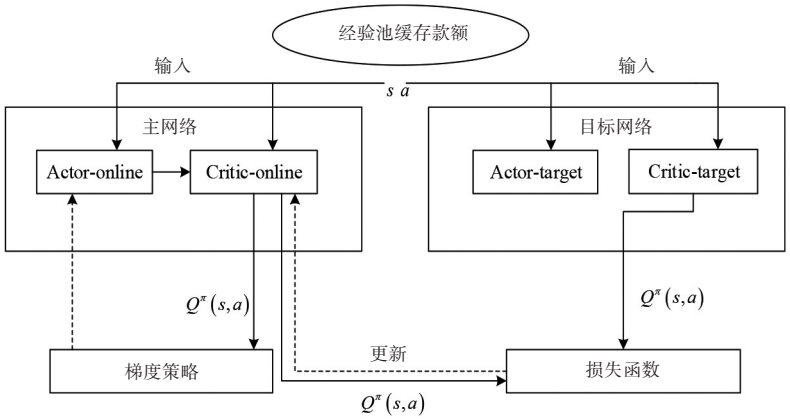


图 2 DDPG 网络结构示意图

Fig. 2 Schematic diagram of the DDPG network

1.2 病历数据加密模型设计

集成 BiLSTM、KV-MemNNs、CRF 以及 DDPG 完成病历敏感信息实体命名后,研究采用 AES 算法进行了数据加密。AES 算法是一种对称密钥加密算法,取代了早期的数据加密标准,可提供更高的安全性。AES 加密和解密使用相同的密钥,并将明文数据划分为固定长度 128 bit 的数据块;AES 支持 128 位、192 位和 256 位的密钥长度,对应需扩展产生 11、13、15 组子密钥,算法工作流程如图 3 所示[12]。

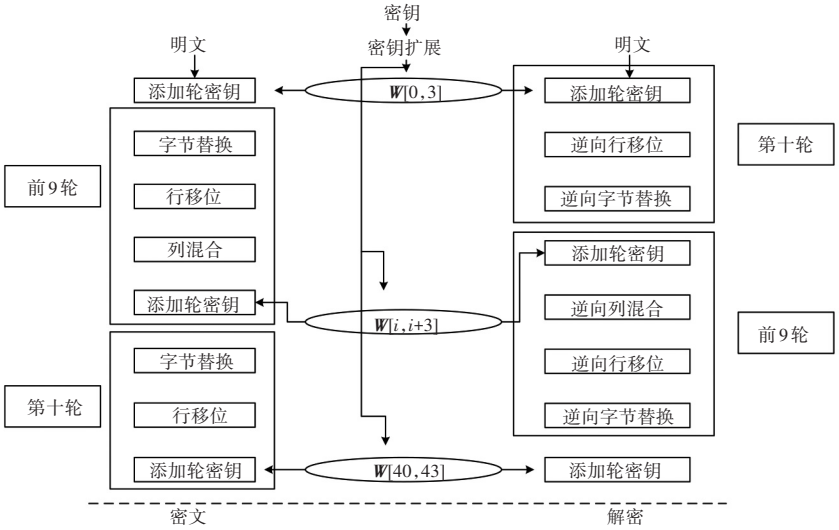


图 3 AES 算法工作流程

Fig. 3 Workflow of the AES algorithm

如图 3 所示,AES 算法通过多轮次的置换网络结构来实现加密过程,每轮操作由字节替换、行移位、列混合和添加轮密钥组成[13]。加解密中每轮的密钥分别由种子密钥经过密钥扩展算法得到。AES 算法的密钥扩展操作是将原始密钥进行字节替换,轮密钥的索引表达式见式(8)。

$$\boldsymbol{W}[4i+j]=\boldsymbol{W}[4(i-1)+j]\oplus\boldsymbol{W}[4i-1+j] \tag{8}$$

式中,$\boldsymbol{W}$ 表示轮密钥矩阵;i j 表示不同轮。轮密钥将在后续的加密轮次中使用,每轮加密均使用不同的密钥,增强算法的安全性。与状态矩阵进行操作的轮密钥的索引表达式见式(9)。

$$\boldsymbol{W}[4i]=\boldsymbol{W}[4(i-1)+j]\oplus g[4i-1+j] \tag{9}$$

式中,g 表示与轮密钥相关的字节序列。AES 算法的字节替换即通过 Substitution box 的固定置换表替换输入数据的每个字节,增加数据的混淆程度;解密过程中则使用 Inverse Substitution box。行移位是将数据块中的每一行进行循环左移,不同行的移动距离不同,进一步扩散数据;逆行移位通过循环右移实现。除最后一轮外,列混合是使用固定矩阵与数据块的每一列进行矩阵乘法运算,进一步混

淆数据。为了确保每轮加密都使用不同的密钥,AES算法通过添加轮密钥将当前轮次的轮密钥与数据块进行异或运算[14-15]。

由于电子病历系统中的数据长度不一,传统的AES算法只能采用相同的处理流程,并不能直接应用于电子病历系统中,研究对AES算法进行改进。首先,研究改进了AES算法的体系结构,将传统的串行处理模式改为异步并行处理模式,将不同的数据块分配给不同的处理单元进行并行处理,并将AES算法轮数设定为7。并将列混合变换进行优化处理,改进的列混合变换见式(10)。

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02(a_0 \oplus a_1) \\ 02(a_1 \oplus a_2) \\ 02(a_2 \oplus a_3) \\ 02(a_0 \oplus a_3) \end{bmatrix} \oplus \begin{bmatrix} a_2 \oplus a_3 \oplus a_1 \\ a_0 \oplus a_3 \oplus a_2 \\ a_0 \oplus a_1 \oplus a_3 \\ a_1 \oplus a_2 \oplus a_0 \end{bmatrix} \tag{10}$$

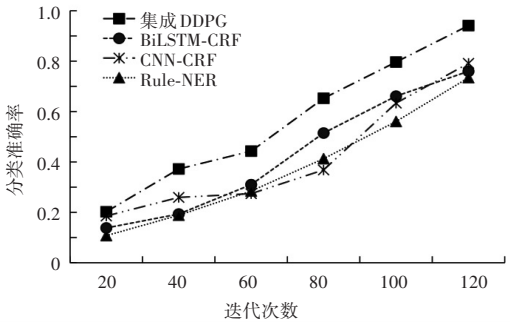
式中,b_i表示列混合变换的输出元素;a_i表示列混合变换的输入元素。式(10)的列变换过程可减少Xtime运算次数。此外,若电子病历所有记录均进行完整的密钥扩展操作,将降低系统性能,因此研究对密钥扩展过程进行了改进。研究在算法外部实施密钥扩展操作,并将扩展结果传送返回AES算法,密钥扩展仅需针对第一条数据展开,节约了算法执行时间。

2 加密模型性能分析

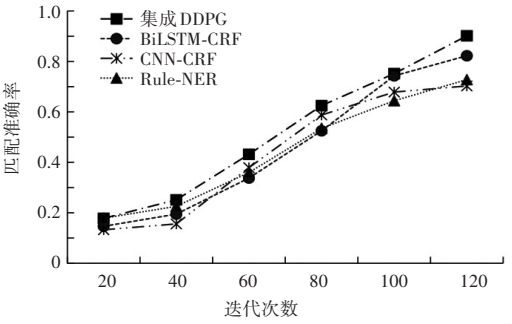
为了验证研究的数据加密模型性能,研究进行了NER算法测试及加密应用分析。实验所使用的操作系统为Window 10 64位系统,中央处理器为Intel i7 10700k,图形处理器为GTX 3060 12G。深度学习框架为Pytorch 1.7,算法实现语言Python3.8。选用文娱NER-Youku、电商NER-Taobao以及简历NER-新浪财经作为实验数据集。NER-Youku由3大类、9小类实体类别构成,训练集8 001条、验证集1 000条、测试集1 001条。NER-Taobao由4大类、9小类实体类别构成,训练数据集6 000条,验证数据集998条,测试数据集1 000条。NER-新浪财经包含1 027份简历摘要,8种命名实体组成。

首先分析NER模型的实体识别性能。对比模型包括传统的BiLSTM-CRF、卷积神经网络CRF(convolutional neural networks CRF, CNN-CRF)以及基于规则的NER(rule-based NER,Rule-NER),实验结果如图4所示。由图4(a)可见,研究设计集成DDPG NER模型分类准确率处于最高水平,随迭代次数增加,最高分类准确率可达0.941。较BiLSTM-CRF、CNN-CRF以及Rule-NER模型分别提升0.181、0.150、0.207。由图4(b)可见,集成DDPG NER模型的实体匹配准确率高达0.901,BiLSTM- CRF、CNN-CRF以及Rule-NER模型的实体匹配准确率取值0.822、0.702、0.727。由图4(c)可见,集成DDPG NER模型在F_1值上仍表现优异,最高取值可达0.876,同等实验环境下,基于DRL的NER模型表现最优,有利于病历数据的加密。

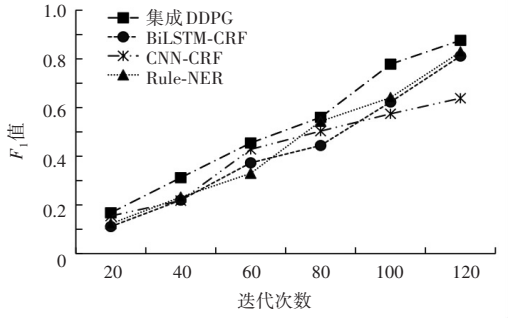
以中国某三甲医院的电子病历库作为实验对象,评估集成DDPG NER模型及改进AES算法的性能,加密算法的对比模型包括传统的AES算法、公钥加密算法(rivest shamir adleman,RSA)以及三重数据加密算法(triple data encryption standard, Triple DES),实验结果如图5所示。由图5(a)可见,集成DDPG NER模型的标准化语义等级(normalized semantic level, NSL)取值最优,可达0.90。BiLSTM-CRF、CNN-CRF以及Rule-NER模型的NSL值仅0.653、0.632、0.707。NSL评估了模型对词汇、句法以及语义的理解能力,评估了实体名称的语义等级,取值越大,实体语义准确性越高。可见,研究的设计对电子病历中的文本信息可准确进行实体命名,方便敏感信息加密。由图5(b)可见,当字节数低于280时,改进的AES加密算法的加密速度保持在100 ms左右。传统AES加密算法的加密耗时一直处于100 ms以上,当字节数高于80时,加密速度高于200 ms左右。RSA算法耗时最多,达到500 ms以上;Triple DES算法加密速度较优,仅次于研究改进的AES加密算法,字节数高于320时为300 ms左右。研究提出的并行策略显著改善了算法的加密速度。



(a) 分类准确率对比



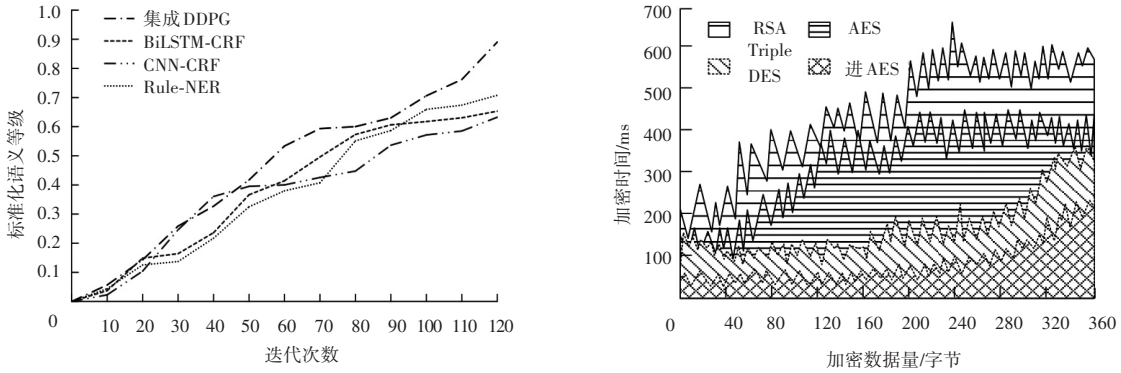
(b) 匹配准确率对比



(c) F_1值对比

图4 不同NER模型性能对比

Fig. 4 Performance comparison of different NER models

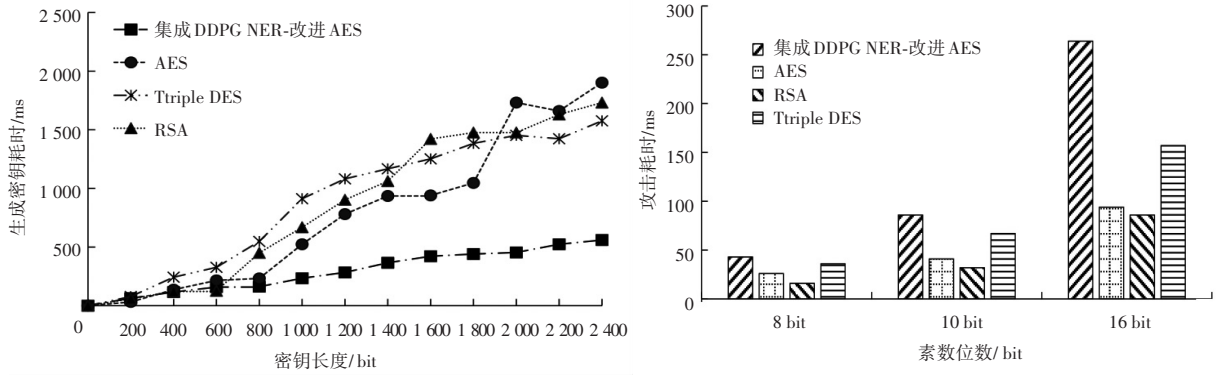


(a) 命名实体对比　　(b) 加密时间对比

图 5　不同算法在电子病历实体识别及加密过程中的性能对比

Fig. 5　Performance comparison of various algorithms in EMR entity recognition and data encryption

进一步对比研究不同加密算法生成密钥耗时,与电子病历加密后的安全性,实验结果如图 6 所示。由图 6(a)可见,研究设计的基于集成 DDPG NER 的改进 AES 算法生成密钥时间最短,在 2 400 bit 的密钥长度内密钥生成时间始终低于 1 000 ms,最多耗时 559. 93 ms。相比 AES 算法、RSA 算法以及 Triple DES 算法,密钥平均生成时间分别降低 488. 732 ms、589. 28 ms、564. 71 ms。图 6(b)中,研究使用了暴力攻击测试不同加密算法抵抗攻击的性能。由图 6(b)可见,研究设计的基于集成 DDPG NER 的改进 AES 算法抵御攻击所消耗的时间在不同素数位数上明显高于其他 3 种算法,其中素数位数为 8 bit 时,基于集成 DDPG NER 的改进 AES 算法的抗攻击时间为 43 s,传统的 AES 算法的抗攻击时间为 26 s,RSA 算法的抗攻击时间为 16 s,Triple DES 算法的抗攻击时间为 36 s。随着素数位数的增加,攻击不同算法的难度均不断增加,加密安全性得到提升。当素数位数为 16 bit 时,基于集成 DDPG NER 的改进 AES 算法的抗攻击时间为 264 s,传统的 AES 算法的抗攻击时间为 94 s,RSA 算法的抗攻击时间为 86 s,Triple DES 算法的抗攻击时间为 157 s。



(a) 生成密钥耗时对比　　(b) 攻击耗时对比

图 6　不同加密算法的应用性能比较

Fig. 6　Application performance comparison of different encryption algorithms

3　结论

医疗数字化、信息化进步推进了电子病历的应用,电子病历共享调阅过程中需严格保护患者的隐私信息。为了减少电子病历隐私泄露、数据滥用风险,研究基于 BiLSTM、KV-MemNNs、CRF 以及深度强化学习技术 DDPG 集成了 NER 模型,并在此基础上利用 AES 算法设计了数据加密模型。实验结果表明,集成 DDPG NER 模型最高分类准确率可达 0. 941,实体匹配准确率高达 0. 901, F_1 值最高取值可达 0. 876。同时该模型的 NSL 取值最高,BiLSTM-CRF、CNN-CRF、Rule-NER 模型的 NSL 值仅 0. 653、0. 632、0. 707,研究基于 DRL 展开加密设计有利于敏感信息的识别。改进的 AES 加密算法加密速度保持在 100 ms 左右,密钥生成最多耗时 559. 93 ms,基于集成 DDPG NER 的改进 AES 算法抵御攻击所消耗的时间在不同素数位数上明显高于其他 3 种算法。研究基于 DRL 与 AES 算法展开的病历数据加密取得了较优表现,但研究并未探究电子病历加密系统在整个医疗系统中流转的完整性与可用性,还需进一步深入探究。

参考文献

[1]李岱高, 刘勤明, 李佳翔. 基于麻雀搜索算法考虑病患流的医院诊疗设备维护优化研究[J]. 上海理工大学学报, 2023, 45(5): 513-522.

(下转第 163 页)