

基于区块链且可验证完整性的电子病历数据 共享方案

李亚红^{1,2}, 李 强¹, 李哲玮¹, 王彩芬³, 杨小东⁴

¹ 兰州交通大学 电子与信息工程学院 兰州 中国 730000

² 电子科技大学 计算机与工程学院 成都 中国 610054

³ 深圳技术大学 大数据与互联网学院 深圳 中国 518118

⁴ 西北师范大学 计算机与工程学院 兰州 中国 730000

摘要 云服务给电子病历数据的共享带来了许多便利, 由于云上数据共享依赖于第三方的云计算基础设施, 外包存储的数据面临着各种安全问题, 如给云服务器带来巨大的存储压力、外包数据可能会面临着被篡改或者丢失删除的威胁。当检索外包的数据时, 用户外包数据中可能包含用户的隐私, 加密的数据无法支持用户细粒度的检索, 这些问题成为云上数据共享服务中亟待解决的。因此本文提出了一种区块链辅助的基于属性的电子病历共享方案, 该方案采用基于属性的加密技术, 在策略隐藏的基础上实现了电子病历数据的机密性和细粒度访问控制。采用可搜索加密技术对多关键字进行加密, 提高了搜索准确度, 并将关键字密文上传到区块链中, 节省了存储开销, 由于区块链的不可篡改性, 保证数据的安全性, 实现了可授权用户对密文的安全搜索。为了防止云服务器向用户返回部分或不正确的密文, 用户与云交互验证了密文的正确性。该算法将大量的运算外包给云服务器, 降低了数据访问用户的计算负担。此外, 功能和安全分析表明, 所提方案满足多种功能安全需求, 并在标准模型下, 基于困难问题证明了方案在选择访问策略和选择明文攻击下具有不可区分性。通过数值和理论分析表明该方案在陷门生成阶段和搜索阶段具有较好计算效率, 极大地提高了多关键字可搜索加密方案的搜索效率。同时, 该方案在具备多特性的情况下存储开销有所减少, 更适用于电子病历的数据共享场景。

关键词 区块链; 云存储; 基于属性的加密; 可搜索加密; 电子病历

中图分类号 TP309.7 **DOI号** 10.19363/J.cnki.cn10-1380/tn.2025.09.10

Blockchain-based Electronic Health Record Data Sharing Scheme with Integrity Verification

LI Yahong^{1,2}, LI Qiang¹, LI Zhewei¹, WANG Caifen³, YANG Xiaodong⁴

¹ School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730000, China

² School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

³ Big Data and Internet Academy, Shenzhen University of Technology, Shenzhen 518118, China

⁴ School of Computer Science and Engineering, Northwestern Normal University, Lanzhou 730000, China

Abstract Cloud services have brought a lot of conveniences to the sharing of electronic medical record data. However, cloud data sharing relies on third-party cloud computing infrastructure, leading to various security issues for outsourced storage data, such as enormous storage pressure on cloud servers, and the threat of tampering or loss and deletion of outsourced data. When retrieving outsourced data, user outsourced data may contain user privacy information, and encrypted data cannot support fine-grained retrieval. These issues have become urgent issues in cloud based data sharing services. In this paper, a blockchain-assisted attribute-based encryption scheme is proposed for electronic medical record sharing. In this scheme, on the basis of policy hiding, confidentiality and fine-grained access control of electronic medical record data are achieved by attribute-based encryption. To save storage costs, using searchable encryption technology to encrypt multi-keywords improves search accuracy, and the keywords ciphertext is uploaded to blockchain. Due to the immutability of the blockchain, data security is ensured, and authorized users can safely search for ciphertext. In order to prevent cloud servers from returning partial or incorrect ciphertext to users, users interact with the cloud to verify the correctness of the

通讯作者: 李亚红, 博士, 副教授, liyahong@lztu.edu.cn

本课题得到国家自然科学基金项目(No. 61663041, No. 61901201, No. 61762058, No. 62002050, No. 61872060, No. 62241207, No. 62262060); 甘肃省科技计划项目(No. 22JR5RA158, No. 22JR5RA350); 甘肃省高校教师创新基金项目(No. 2023A-041, No. 2023-ZD-234); 甘肃省教育厅产业支撑计划项目(No. 2022CYZC-17); 甘肃省教育厅高校创新基金项目(No. 2023A-041); 2023年度兰州市科技发展计划项目(No. 2023-ZD-234)资助。

收稿日期: 2023-10-10; 修改日期: 2024-03-07; 定稿日期: 2025-08-14

ciphertext. To reduce the computational burden on data access users, this algorithm outsources a large amount of computation to cloud servers. In addition, functional and safety analysis indicate that the proposed scheme meets functional security requirements. Under the random oracle model, based on the decisional q -parallel BDHE assumption, it is proved that the scheme can guarantee the security of indistinguishability against selective access policy and chosen plaintext attacks. Numerical analysis indicates that the scheme has better computational efficiency in the trapdoor generation stage and search stage, greatly improving the search efficiency of multi keywords searchable encryption schemes. Meanwhile, the storage cost is reduced when the scheme has multi-features which are suitable for data sharing scenarios in electronic health records.

Key words cloud storage; attribute-based encryption; searchable encryption; electronic health record

1 引言

随着医疗信息技术的快速发展, 现代医疗卫生系统通过电子病历(electronic health record, EHR)来收集、分析和远程监控患者的就医数据, 其中包含了患者的身份信息、联系方式、健康状况等敏感数据。传统的 EHR 是将数据存储在医院本地服务器, 在占用大量设备的同时, 也不便于数据共享^[1]。为了节省本地的存储开销, 将这些数据存储云平台中, 以供医生、研究机构、保险公司和其他部门访问。但云是半可信的, 导致敏感数据泄露或未经授权的访问等安全问题, 因此, 如何在云环境中实现高效且安全的数据的访问、细粒度的数据共享以及用户隐私信息的保护是当前一项重大挑战。

为了保证 EHR 数据安全, 需在上传云服务前对数据进行加密处理, 云一方面为用户提供存储服务, 另一方面也需要提供数据检索服务。然而传统的搜索机制很难实现对密文数据的检索。可搜索加密(Searchable Encryption, SE)的提出有效地解决了这一问题。Song 等人^[2]利用对称加密算法对文档加密, 为用户通过关键词从外包数据库中检索加密数据提供了技术支持。Boneh 等人^[3]基于双线性对构建了公钥可搜索加密方案, 实现了密文关键词检索。此后, 众多学者提出了具有不同特性的搜索方案, 如单关键词搜索、多关键词搜索、模糊关键词搜索等。在实际应用中, 单关键词的密文检索有一定的局限性, 如单关键词搜索将返回一些不相关的文件, 导致大量的通信开销和存储冗余, 而多关键字搜索可以准确定位搜索的目标文件, 因此具有更好的应用场景。Fan 等人^[4]提出了一种支持多关键词的可搜索加密方案, 允许用户进行多关键词搜索的同时可验证搜索结果的正确性。Babu 等人^[5]提出一种基于哈希树的多关键词搜索方案, 利用哈希树技术, 保证用户在不泄露数据隐私的情况下进行搜索。Sun 等人^[6]提出了一种支持多关键字检索的文本搜索加密方案。该方案使用基于词频的搜索索引和余弦相似性的向量空间模型对搜索结果进行排序, 实现了较高的搜索

精度。

随着云服务的应用越来越广泛, 用户的需求也不断的与日俱增, 为了满足密文是可被检索的同时保证细粒度访问控制, 基于属性的加密技术得到了广泛的关注。属性加密^[7](Attribute-based Encryption, ABE)可根据用户属性来控制数据访问权限, 能够更好地保证患者数据的隐私性和安全性。结合 SE 和属性加密技术的基于属性的 SE 方案不仅可以实现关键字的搜索, 还可以有效解决隐私数据的访问控制问题。Li 等人^[8]提出一种基于属性的多关键字搜索方案, 在保证数据隐私的情况下, 对加密数据进行多关键词搜索, 但该方案不适用于多用户场景。Yin 等人^[9]提出一种轻量级可搜索医疗数据共享方案, 该方案在支持关键字搜索和策略隐藏的基础上采用大属性域和线性秘密共享结构。文献[10]提出一种基于属性的多关键词搜索加密方案, 用于在多用户的场景中加密电子病历, 但该方案计算效率较低, 因此不适用于大规模数据的加密。大多属性基的 SE 方案都采用云存储^[11-12]。Xu 等人^[13]提出一种基于属性的关键词搜索方案, 用于云环境中保护用户隐私和数据安全, 该方案支持策略隐藏。Miao 等人^[14]的方案引入访问控制机制, 用户可通过属性来访问密文数据, 同时该方案还考虑了数据的动态更新和属性撤销问题。Li^[15]提出了一个基于云辅助 eHealth 系统属性值类型数据库的多用户密态医疗数据检索方案, 对患者的病例生成标签存储在云服务器保存的三层字典中。在 ABE 方案中, 访问控制越精细, 所需的计算成本越高。为了降低这种开销, 可在不泄露数据信息的情况下将昂贵的计算任务交付给云执行计算。Liu 等人^[16]结合云技术和属性加密, 对共享文件的数据生成标签, 可实现重复数据的删除。Belguith 等人^[17]设计出一种云环境下基于属性的加密方案, 将解密计算外包给云服务器, 提高了解密效率。

上述方案实现了云环境下的数据共享和存储, 但是云服务器是诚实但好奇的, 它在完成搜索任务的同时, 可能试图从搜索请求以及返回的搜索结果等数据中分析提取一些敏感信息, 给 EHR 共享的数

据带来泄露的风险。区块链其去中心化的分布式存储结构,能够保证存储的数据不被篡改,可适用于电子病历的数据共享。Yang 等人^[18]提出一种基于区块链和云边端协同的电力数据共享方案。该方案利用区块链不可篡改的特性,将用户属性与数据哈希值上链存储。Niu 等人^[19]基于区块链的多关键字属性基可搜索加密方案,结合区块链的智能合约技术,保证了在方案中三方的公平性。Liu 等人^[20]基于区块链技术提出了一个可搜索属性基加密方案,该方案结合智能合约技术使用区块链取代属性基加密方案中的可信中心,从而达到去中心化的目的。文献[21]提出了区块链上基于云辅助的属性基可搜索加密方案,利用区块链不可篡改的特性确保关键字密文的安全。Su 等人^[22]提出了一种基于属性的云链协同存储的 EHR 方案,且可实现查询结果的排序功能。Wang 等人^[23]提出群组内基于区块链的匿名可搜索加密方案,利用智能合约的可信性,在用户验证搜索结果正确后向云服务器支付搜索费用,解决了用户与云服务器之间的公平支付问题。文献[24]提出一种多关键字搜索的可搜索加密方案,结合区块链智能合约技术,利用区块链的不可篡改性,保证了搜索的公平性。

本文以 EHR 的安全存储、隐私保护和安全共享为目标,将可搜索加密和属性加密技术结合区块链应用于 EHR,主要工作和贡献有以下两点:

(1) 本文设计了一个属性基多关键字可搜索加密方案,以实现了对加密数据的有效搜索和细粒度访问授权,将加密的关键字密文上传至区块链,由区块链完成搜索,区块链不可篡改的特性可确保关键字密文的安全性,同时保证了只有当数据用户的属性集满足访问策略并且关键字匹配时,区块链才能够返回搜索结果。

(2) 密文完整性验证。当数据被外包在云服务器后,外包数据可能会面临着被篡改或者丢失删除的威胁。因此为了防止云服务器向用户返回部分或不正确的密文,数据属主生成了数据密文的签名,并存储在云服务器中,用户可验证密文签名的正确性,保证数据共享的正确性。同时本方案支持外包解密,大部分解密计算的工作委托给云服务器执行,降低了数据访问用户的计算负担。

2 相关知识

2.1 双线性映射

设 G_1 和 G_2 为阶数为 p 的两个乘法循环群。定义

双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 具有以下性质。

(1) 双线性: 对任意的 $g_1, g_2 \in G_1$, 随机选择 $a, b \in Z_p^*$, 都有 $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ 。

(2) 非退化性: 存在 $g \in G_1$, 使 $e(g, g) \neq 1$ 。

(3) 可计算性: 对任意的 $g_1, g_2 \in G_1$, 存在一个有效算法计算 $e(g_1, g_2)$ 。

2.2 判定性 q -parallel BDHE 困难假设

设 G_1 是阶数为 p 的群, g 是群 G_1 的生成元, 随机选择 $s, a, b_1, \dots, b_q \in Z_p^*$ 。若给定敌手 $\mathcal{A}$ 的参数

$$\begin{aligned} \text{PP} = \{ & G, p, q, g, g^s, g^a, \dots, g^{(a^q)}, g^{(a^{q+2})}, \dots, g^{(a^{2q})}, \\ & g^{sb_1}, g^{(a/b_1)}, \dots, g^{(a^q/b_1)}, g^{(a^{q+2}/b_1)}, \dots, g^{(a^{2q}/b_1)} \\ & g^{(a \cdot s \cdot b^k/b_j)}, \dots, g^{(a^q \cdot s \cdot b^k/b_j)} \}_{1 \leq j, k \leq q, k \neq j} \end{aligned}$$

敌手 $\mathcal{A}$ 将无法区分 $e(g, g)^{a^{q+1}s}$ 与随机元 $R \in G_2$ 。敌手 $\mathcal{A}$ 在 q -parallel BDHE 问题上取得的优势为:

$$\left| \Pr[\mathcal{A}(\text{PP}, e(g, g)^{a^{q+1}s}) = 0] - \Pr[\mathcal{A}(\text{PP}, R) = 0] \right| \leq \varepsilon。$$

如果敌手 $\mathcal{A}$ 在任何多项式时间内不存在以不可忽略的优势来解决判定性 q -parallel BDHE 问题, 则称判定性 q -parallel BDHE 假设在群 G_1 上成立。

2.3 访问结构

设 $\{P_1, P_2, \dots, P_n\}$ 是一个基于属性加密方案的属性集合, 对于集合 $A \subseteq 2^{\{P_1, P_2, \dots, P_n\}}$ 。对任意的 U, V , 如果 $U \in A$ 且 $U \subseteq V$, 那么 $V \in A$, 若上述关系成立, 则称 A 是单调的。一个访问结构 A 就是由 $\{P_1, P_2, \dots, P_n\}$ 的非空属性子集构成的集合。在 A 中的集合被称为授权访问集合, 不在 A 中的集合称为非授权访问集合。

2.4 线性秘密分享方案

给定属性集 ATT , 定义一个线性秘密分享方案 Γ , 则存在一个单调的访问结构 (A, ρ) , 其中 A 是一个 l 行 n 列的共享生成矩阵, ρ 将矩阵 A 中的第 i 行映射到属性集 ATT 中。线性秘密分享方案由以下两个算法构成。

线性共享: 当矩阵 A 分享一个秘密值 $s \in Z_p$ 时, 首先随机选择 $v_2, \dots, v_n \in Z_p$, 定义向量 $\vec{v} = (s, v_2, \dots, v_n)$, 得到 $\vec{\lambda} = A \cdot \vec{v} = (\lambda_1, \lambda_2, \dots, \lambda_l)^T$ 作为 s 的秘密共享份额, 其中 $\lambda_i \in \rho(i)$ 。

重构秘密值: 该算法用于从秘密共享中重构 s 。

设 S 是任意授权集合, 且 $I = \{i : \rho(i) \in S\} \subseteq [1, l]$, 如果存在一个常数集 $\{w_i \in \mathbb{Z}_p\}_{i \in I}$, 使 $\sum_{i \in I} w_i A_i = (1, 0, \dots, 0)$, 从而有 $\sum_{i \in I} w_i \lambda_i = s$ 。

3 系统模型与安全模型

3.1 系统模型

整个模型由五个实体构成, 包括属性授权机构、数据属主、数据用户、区块链以及云服务器, 方案的系统模型如图 1 所示。

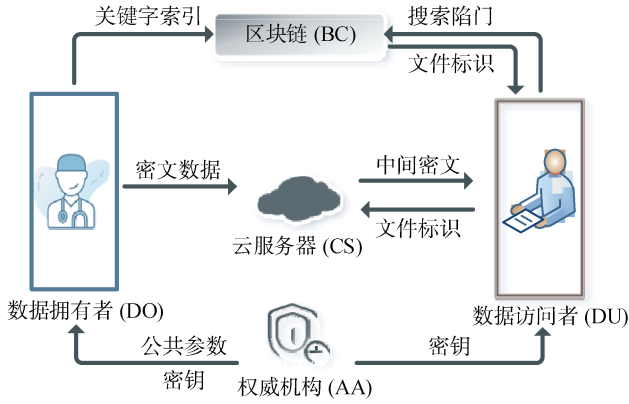


图 1 系统模型

Figure 1 System model

属性权威机构(Attribute Authority, AA): AA 为一个全局可信机构, 负责系统的建立, 生成系统参数以及主密钥, 并且根据用户提供的属性生成私钥。

数据属主(Data Owner, DO): DO 可以是医生或医院, 为患者生成电子病历 EHR, 并构造相应的访问策略, 将加密后的 EHR 通过安全信道上传到云服务器。同时将关键字密文存储在区块链中。

数据用户(Data User, DU): DU 用其私钥和感兴趣的关键词产生搜索陷门, 并将陷门上传至区块链。解密时, DU 发送盲化属性密钥给云服务器, 云服务器进行部分解密, 最后由 DU 进行二次解密得到明文。

区块链(Block Chain, BC): BC 存储 DO 的访问策略和关键词索引, 验证 DU 上传的搜索陷门与关键词索引是否匹配。若匹配, 则搜索成功, 区块链节点将文件的标识符返回给 DU。

云服务器(Cloud Server, CS): CS 负责存储 EHR 的密文。当关键字搜索成功后, CS 与 DU 交互, 验证 CS 返回给 DU 的密文是否正确。若正确, 云服务器进行部分解密, 并将部分解密的密文分发给 DU。

3.2 算法形式化定义

本文方案共有 7 个算法组成, 包括系统初始化、密钥生成、数据加密、陷门生成、密文搜索、验证和密文解密。

系统初始化 $\text{Setup}(1^\lambda, \text{ATT}) \rightarrow (\text{Param}, \text{MSK})$: 给定安全参数 λ , 属性集 ATT 和一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$, AA 输出系统公开参数 Param, 保存系统主密钥 MSK。

密钥生成算法 $\text{KeyGen}(\text{Param}, \text{MSK}, \text{uid}, S_{\text{uid}}) \rightarrow \text{RK}$: 输入系统公开参数 Param, 用户身份标识 uid 以及其属性集 S_{uid} , AA 运行此算法输出 DU 的属性密钥 RK 和 DO 的公私钥。

加密算法 $\text{Encrypt}(\text{Param}, k, (A, \rho), \text{KW}, F) \rightarrow (\text{CT}, \{C_i\}_{i \in [1, m]}, \{\text{sig}_i\}_{i \in [1, m]}, I)$, 有以下三个步骤。

(1) 文件加密: 输入系统公钥 Param、对称密钥 k 和文件集 $F = \{f_1, f_2, \dots, f_m\}$, DO 输出文件的密文 $\{C_1, C_2, \dots, C_m\}$ 和对应密文的签名 $\{\text{sig}_1, \text{sig}_2, \dots, \text{sig}_m\}$ 。

(2) 对称密钥加密: 输入参数 Param、访问结构 (A, ρ) , 输出对称密钥的密文 CT。

(3) 关键词加密算法: 输入参数 Param、关键词集 KW 和 DO 的私钥, 输出关键词索引 I。

陷门生成算法 $\text{TrapGen}(\text{KW}', \text{Param}) \rightarrow \text{TP}$: 输入公共参数 Param 和要查询的关键词集 KW', DU 运行此算法输出陷门 TP。

密文搜索 $\text{Search}(I, \text{TP}, S_{\text{uid}}) \rightarrow \text{id}$: 输入关键词索引 I、搜索陷门 TP 和 DU 的属性 S_{uid} , 如果搜索成功, 输出相关文件标识符 id 给 DU, 否则, 算法终止。

验证 $\text{Verify}(\text{Param}, \text{id}, \text{sig}_i, C_i) \rightarrow 1/0$: 输入搜索返回的文件标识 id, 验证此次搜索结果是否正确, 若正确则输出 1, 完成搜索, 否则返回 0, 搜索失败, 终止此次搜索。

密文解密由三部分算法构成。

(1) 部分密钥 $\text{Transform}(\text{RK}) \rightarrow \text{tpk}$: 输入属性密钥 RK, 输出部分密钥 tpk。

(2) 部分密文解密 $\text{Decrypt}_1(\text{tpk}, \text{CT}) \rightarrow \text{IC}$: 输入中间密钥 tpk 和密文 CT, 此算法输出部分密文 IC。

(3) 密文解密 $\text{Decrypt}_2(\text{IC}) \rightarrow F$: 输入部分密文 IC, 运行此算法, 解密得到明文。

3.3 安全模型

通过概率多项式时间攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏来定义: 针对选择访问策略和选择明文攻击下的不可区分性 (Indistinguishability against Selective

AccessPolicy and Chosen Plaintext Attacks, IND-SAP-CPA)。

初始化: $\mathcal{A}$ 将任意的挑战访问策略 (A^*, ρ^*) 给挑战者 $\mathcal{C}$ 。

系统建立: 输入安全参数 λ , $\mathcal{C}$ 运行 $\text{Setup}(1^\lambda, \text{ATT})$ 算法得到 $(\text{Param}, \text{MSK})$, 将 Param 发送给 $\mathcal{A}$, 保留 MSK 。

阶段 1: 在此阶段 $\mathcal{A}$ 适应性地进行多项式有界次下列询问:

密钥询问: 攻击者 $\mathcal{A}$ 询问关于属性集 $(\text{uid}, S_{\text{uid}})$ 密钥, $\mathcal{C}$ 运行 KeyGen 算法返回相应的私钥给 $\mathcal{A}$ 。

中间密钥询问: 输入属性集 $(\text{uid}, S_{\text{uid}})$ 。 $\mathcal{C}$ 在表 V 中查找 $(S_{\text{uid}}, \text{RK}_{\text{uid}}, \text{tpk})$, 其中 tpk 为中间解密密钥。如果存在则直接将密钥传送给 $\mathcal{A}$, 否则 $\mathcal{C}$ 运行 KeyGen 和 Transform 算法, 将 $(S_{\text{uid}}, \text{RK}_{\text{uid}}, \text{tpk})$ 存储在 V 中, 再将 tpk 发送给 $\mathcal{A}$ 。

挑战: $\mathcal{A}$ 选择两个相同长度的消息 k_0 和 k_1 , 任何查询的属性集都不能满足这个访问结构 (A^*, ρ^*) 。 $\mathcal{C}$ 随机选择 $b \in \{0, 1\}$ 并在访问结构 (A^*, ρ^*) 加密消息 k_b 得到挑战密文 CT_b , 将 CT_b 发送给 $\mathcal{A}$ 。

阶段 2: $\mathcal{A}$ 可以进行同阶段 1 相同的询问。

猜测: $\mathcal{A}$ 输出猜测 $b' \in \{0, 1\}$ 。如果 $b = b'$, 则 $\mathcal{A}$ 赢得了此游戏。

攻击者 $\mathcal{A}$ 赢得这个游戏的优势定义为

$$\text{Adv}_{\mathcal{A}} = \left| \Pr(b' = b) - \frac{1}{2} \right|$$

如果在概率多项式时间内攻击者在上述游戏 $\mathcal{A}$ 中获胜的概率可忽略, 那么本文方案是 IND-SAP-CPA 安全的。

4 方案构造

本方案设计的主要算法过程如下:

系统初始化:

给定安全参数 λ 和属性集 ATT 。该算法由 AA 执行: 选择阶数为 p 的两个乘法循环群 G_1 和 G_2 , G_1 的生成元为 g , 定义双线性映射 $e: G_1 \times G_1 \rightarrow G_2$, 定义三个哈希函数 $H_1: \{0, 1\}^* \rightarrow G_1$, $H_2: \{0, 1\}^* \rightarrow Z_p^*$, $H_3: \{0, 1\}^* \times \{0, 1\}^* \rightarrow Z_p^*$ 。然后随机选择 $\alpha, \beta \in Z_p$, 计算 g^α 、 g^β 和 $e(g, g)^\alpha$ 。对属性集 ATT 中的每一个属性 $i \in \text{ATT}$, 随机选择 $v_i \in Z_p$, 计算 g^{v_i} 。选择对称加密体制 AES , 用 $\text{Enc}()$ 和 $\text{Dec}()$ 分别表示 AES 的加

密算法和解密算法。输出公共参数 $\text{Param} = \{G_1, G_2, g, e, H_1, H_2, H_3, g^\alpha, \{g^{v_i}\}_{i \in \text{ATT}}, e(g, g)^\alpha, g^\beta, \text{Enc}(), \text{Dec}()\}$, 主密钥 $\text{MSK} = (\alpha, \beta, \{v_i\}_{i \in \text{ATT}})$ 。

密钥生成:

该算法由 AA 执行, 输入主密钥 MSK , AA 根据用户身份标识符 uid 和属性集 $S_{\text{uid}} = \{A_1, A_2, \dots, A_q\}$ 生成用户的密钥, 其中 $\text{uid} \in \{0, 1\}^*$ 。 AA 具体操作如下:

(1) 随机选择 $\tau_1 \in Z_p$, 计算 DO 的公私钥 $\text{pk}_1 = g^{\tau_1}, \text{sk}_1 = \tau_1$ 。

(2) 随机选择 $\tau_2 \in Z_p$, 计算 DU 的公私钥 $\text{pk}_2 = g^{\tau_2}, \text{sk}_2 = \tau_2$ 。

(3) 随机选择 $t \in Z_p$, 计算 DU 的属性密钥 RK : $\text{RK} = (K_0, \{K_{i,1}, K_{i,2}\}_{A_i \in S_{\text{uid}}})$, 其中 $K_0 = H_1(\text{uid})^t$, 对任意的 $A_i \in S_{\text{uid}}$, $K_{i,1} = g^\alpha H_1(\text{uid})^{v_i t}$, $K_{i,2} = H_1(A_i)^\beta$ 。

(4) 通过一个安全的信道分别将 sk_1 和 (RK, sk_2) 传送给 DO 和 DU 。

加密阶段:

该算法由 DO 执行, 分别对数据 EHR 、对称密钥和关键字进行加密。给定公共参数 Param 、 EHR 的文件集 $F = \{f_1, f_2, \dots, f_m\}$, 定义 $\{\text{id}_i\}_{i \in [1, m]}$ 为文件 $\{f_i\}_{i \in [1, m]}$ 的文件标识符。给定访问策略 (A, ρ) , 其中 A 是一个 l 行 n 列的共享生成矩阵, ρ 将矩阵 A 中的第 i 行 A_i 映射到属性集 $\rho(i)$ 的映射中, 每个属性在矩阵 A 中都有唯一的行与之对应。

(1) 数据加密: 选择一个 AES 加密体制内的对称密钥 k , 利用对称加密算法 $\text{Enc}_k()$ 对文件 $\{f_i\}_{i \in [1, m]}$ 加密得到密文 $\{C_i\}_{i \in [1, m]}$ 。为了保证密文的正确性, 生成密文 $\{C_i\}_{i \in [1, m]}$ 的签名集合 $\text{sig} = (\text{sig}_1, \text{sig}_2, \dots, \text{sig}_m)$, 其中 $\text{sig}_i = \left\{ g^{\alpha H_2(\text{id}_i)} \cdot g^{C_i} \right\}_{i \in [1, m]}^{\tau_1}$ 。

(2) 对称密钥加密: DO 根据定义访问策略 (A, ρ) , 随机选择 $s \in Z_p$ 作为秘密共享值, 选择随机数 $v_2, \dots, v_n \in Z_p$, 设向量 $\vec{v} = (s, v_2, \dots, v_n)$, 计算 $\vec{\lambda} = A \cdot \vec{v} = (\lambda_1, \lambda_2, \dots, \lambda_l)^T$ 作为 s 的秘密共享份额。如下计算对称密钥 k 的密文: 随机选择 $r_1, r_2, \dots, r_l \in Z_p^*$, 计算 $C = k \cdot e(g, g)^{\alpha s}$, $C_{1,i} = g^{r_i} g^{\lambda_i}$, $C_{2,i} = g^{r_i}$, $C_{3,i} = g^{v_{\rho(i)} r_i}$, 记 $\text{CT} = (C, \{C_{1,i}, C_{2,i}, C_{3,i}\}_{i \in [1, l]})$ 。

(3) 关键词加密: DO 从数据文件 $F = \{f_1,$

$f_2, \dots, f_m$ 中提取关键词集 $KW = \{kw_1, kw_2, \dots, kw_l\}$, 将其加密并生成关键字索引, 过程如下:

a) 随机选择 $k_1 \in Z_p$, 计算 $l_1 + 1$ 次多项式:

$$f(x) = \prod_{i=1}^{l_1} (x - H_3(kw_i \| pk_2^{sk_1})) (x - k_1) + 1 = \prod_{i=0}^{l_1+1} t_i x^i$$

b) 随机选择 $\chi \in Z_p$, 计算 $I_0 = g^\chi$, $I_i = g^{\chi t_i}$, $i = 0, \dots, l_1 + 1$, 关键词的索引为 $I = (I_0, \{I_i\}_{i \in [0, l_1+1]})$ 。

(4) 属性隐藏: 为了保护 DO 的隐私性, 将访问策略中的属性信息 $A_i \in S_{uid}$, 表示为 $q_i = e(H_1(A_i), g^\beta)$ 。

最后将对称密钥 k 的密文 CT、文件的密文 $\{C_i\}_{i \in [1, m]}$ 以及签名 sig 通过安全通道上传至云服务器。将索引 $I = (I_0, \{I_i\}_{i \in [0, l_1+1]})$ 和 $\{q_i\}_{A_i \in S_{uid}}$ 存储在区块链上。

陷门生成:

当 DU 想要浏览 DO 的病历信息时, 必须生成一个搜索陷门。DU 选择所要搜索的关键字集 $KW' = \{kw'_1, kw'_2, \dots, kw'_l\}$, 随机选择 $c \in Z_p$, 计算 $D = g^c$, $B_i = \frac{1}{l_2} c \sum_{j=1}^{l_2} H_3(kw_j \| pk_1^{sk_2})^i$, $i = 0, \dots, l_1 + 1$ 。对任意的属性 $A_i \in S_{uid}$, 计算 $q'_i = e(g, K_{i,2})$ 。最后 DU 将 $TP = (D, \{B_i\}_{i \in [0, l_1+1]})$ 和 $\{q'_i\}_{A_i \in S_{uid}}$ 上传至区块链。

密文搜索阶段:

给定 DU 的属性集合 S_{uid} 和陷门 TP, 区块链执行该算法对关键字密文进行搜索, 在整个搜索过程中, 不会泄露有关数据文件和所要搜索关键字的有用信息。过程如下。

(1) 由区块链上的共识节点验证等式 $q_i = q'_i$ 是否相等。若不相等, 则说明 DU 的属性不满足访问策略 (A, ρ) , 停止搜索。

(2) 若相等, 验证等式 $e(\prod_{i=0}^{l_1} I_i^{B_i}, g) = e(I_0, D)$ 是否相等。若等式成立, 则说明搜索成功, 并返回文件标识符 $\{id_i\}_{i \in [1, m]}$ 给 DU。此时, 交易有效, 向其他节点广播交易请求。当收到 $\frac{2}{3}$ 的授权后, 接受交易。若等式不成立, 返回搜索失败。

验证阶段:

该算法由 DU 和云服务器交互执行, 用来验证密文的正确性。

(1) 随机选择 $\xi_1, \xi_2, \dots, \xi_m \in Z_p^*$, 将 $\{\xi_i\}_{i \in [1, m]}$ 通过一个安全的信道发送给云服务器。

(2) 云服务器计算 $\eta = \prod_{i=1}^m (\text{sig}_i)^{\xi_i}$ 和 $\bar{\chi} = \sum_{i=1}^m \xi_i C_i$ 。

将 η 和发送给 $\bar{\chi}$ 给 DU。

(3) DU 计算 $Q = g^{\alpha \sum_{i=1}^m H_2(id_i) \xi_i} \cdot g^{\bar{\chi}}$, 验证等式 $e(\eta, g) = e(Q, pk_1)$ 是否相等。若等式相等, 则云服务器存储的密文 $\{C_i\}_{i \in [1, m]}$ 是正确的, 并将密文交由云服务器进行外包解密。否则, 返回错误信息给云服务器, 终止解密。

解密阶段:

此算法分别由云服务器和 DU 执行。首先 DU 盲化属性密钥, 得到部分密钥, 然后交由云服务器对密文 CT 进行部分解密得到部分密文 IC, 最后 DU 对部分密文 IC 二次解密得到文件。

(1) 部分密钥生成: DU 随机选择 $d \in Z_p$, 计算中间密钥 $\text{tpk} = (\text{tpk}_1, \text{tpk}_2, \text{tpk}_3)$, 其中 $\text{tpk}_1 = \{K_{i,1}^d\}_{A_i \in S_{uid}}$, $\text{tpk}_2 = g^{\alpha d}$, $\text{tpk}_3 = K_0^d$ 。DU 将 tpk 发送给云服务器, 秘密保存 d 。

(2) 部分解密: 当云服务器接收 tpk 后, 首先验证 DU 的属性集合是否满足访问策略 (A, ρ) , 若不满足, 则终止解密; 否则执行如下的密文外包解密计算:

a) 令 $I = \{i, \rho(i) \in S_{uid}\}$, 存在一组数组 $\{w_i \in Z_p\}_{i \in I}$, 使 $\sum_{i \in I} w_i \lambda_i = s$ 。

b) 计算 $R = \frac{e(\text{tpk}_2, C_{1,i}) e(\text{tpk}_3, C_{3,i})}{e(\text{tpk}_1, C_{2,i})}$ 其中 $i \in I$ 。

c) 计算中间密文 $IC = \prod_{i \in I} R^{w_i}$

d) 将中间密文 IC 和密文 C 发送给 DU。

(3) 密文解密: DU 收到中间密文 IC 和密文 C 后, 执行如下解密操作:

a) 计算 AES 的对称密钥

$$k = \frac{C}{\frac{1}{IC^d}}$$

b) 利用对称密钥 k 和解密算法 Dec() 对 DO 的文件进行解密, 获得文件明文。

5 方案分析

5.1 正确性分析

(1) 搜索阶段的验证:

$$\begin{aligned}
e\left(\prod_{i=0}^{l_1+1} I_i^{B_i}, g\right) &= e\left(\prod_{i=0}^{l_1+1} I_0^{t_i B_i}, g\right) \\
&= e\left(g^{\chi \sum_{i=0}^{l_1+1} \frac{1}{t_i} \sum_{j=1}^{l_2} H_3(\text{kw}_j \| \text{pk}_1^{\text{sk}_2})^i}, g\right) \\
&= e(g, g)^{\frac{1}{t_2} \chi^c \sum_{i=0}^{l_1+1} t_i \sum_{j=1}^{l_2} H_3(\text{kw}_j \| \text{pk}_1^{\text{sk}_2})^i} \\
&= e(g, g)^{\frac{1}{t_2} \chi^c \sum_{i=0}^{l_1+1} \sum_{j=1}^{l_2} t_i (H_3(\text{kw}_j \| \text{pk}_1^{\text{sk}_2}))} \\
&= e(g, g)^{\frac{1}{t_2} \chi^c \sum_{j=1}^{l_2} t (H_3(\text{kw}_j \| \text{pk}_2^{\text{sk}_1}))} \\
&= e(g, g)^{\chi^c} \\
&= e(g^\chi, g^c) \\
&= e(I_0, D)
\end{aligned}$$

(2) 签名阶段的验证:

$$\begin{aligned}
e(\eta, g) &= e\left(\prod_{i=1}^m (\text{sig}_i)^{\xi_i}, g\right) \\
&= e\left(\prod_{i=1}^m ((g^{\alpha H_2(\text{id}_i)} \cdot g^{C_i})^{\tau_i})^{\xi_i}, g\right) \\
&= e\left(\prod_{i=1}^m g^{\alpha H_2(\text{id}_i) \xi_i} \cdot g^{\xi_i C_i}, g^{\tau_i}\right) \\
&= e\left(g^{\sum_{i=1}^m \alpha H_2(\text{id}_i) \xi_i} \cdot g^{\bar{\chi}}, g^{\tau_i}\right) \\
&= e(Q, \text{pk}_1)
\end{aligned}$$

(3) 解密阶段的正确性验证:

因为

$$\begin{aligned}
R &= \frac{e(g^{\alpha d}, g^{\lambda_i} g^{r_i}) e(H_1(\text{uid})^{dt}, g^{v_{p(i)} r_i})}{e(g^{\alpha d} H_1(\text{uid})^{v_i dt}, g^{r_i})} \\
&= \frac{e(g, g)^{\alpha \lambda_i d} e(g, g)^{\alpha d r_i} e(H_1(\text{uid}), g)^{d v_{p(i)} r_i t}}{e(g, g)^{\alpha d r_i} e(H_1(\text{uid}), g)^{d v_{p(i)} r_i t}} \\
&= e(g, g)^{\alpha \lambda_i d}
\end{aligned}$$

故

$$\begin{aligned}
\text{IC} &= \prod_{i \in I} R^{w_i} \\
&= \prod_{i \in I} e(g, g)^{\alpha \lambda_i d w_i} \\
&= e(g, g)^{\alpha d \sum_{i \in I} \lambda_i w_i} \\
&= e(g, g)^{\alpha s d}
\end{aligned}$$

从而

$$\frac{C}{\text{IC}^{\frac{1}{d}}} = \frac{k \cdot e(g, g)^{\alpha s}}{[e(g, g)^{\alpha s d}]^{\frac{1}{d}}} = k$$

5.2 安全性分析

定理 1 如果 q -parallel BDHE 假设成立, 本文的方案也是 IND-SAP-CPA 安全的。

证明: 如果有一个敌手 $\mathcal{A}$ 在选择明文攻击模型下能以不可忽略的优势攻破本文的方案, 则可以构建一个模拟者 $\mathcal{B}$ 以不可忽略的优势攻破文献[25]方案。模拟过程如下:

初始化: $\mathcal{A}$ 将欲挑战的访问结构 (A^*, ρ^*) 发送给 $\mathcal{B}$, 其中 A^* 是 l 行 n 列矩阵。 $\mathcal{B}$ 将其发送给 $\mathcal{C}$ 。 $\mathcal{C}$ 接收到访问结构 (A^*, ρ^*) , 将 Param' 返回给 $\mathcal{B}$, 其中 $\text{Param}' = \{G_1, G_2, g, e, g^\alpha, \{g^{v_i}\}_{i \in \text{ATT}}, e(g, g)^\alpha\}$ 。然后 $\mathcal{B}$ 选择 $\beta \in Z_p$ 和 $H_1: \{0, 1\}^* \rightarrow G_1$, $H_2: \{0, 1\}^* \rightarrow Z_p^*$, $H_3: \{0, 1\}^* \times \{0, 1\}^* \rightarrow Z_p^*$, 将 Param 发送给 $\mathcal{A}$, 其中 $\text{Param} = \{G_1, G_2, g, e, H_1, H_2, H_3, g^\alpha, \{g^{v_i}\}_{i \in \text{ATT}}, e(g, g)^\alpha, g^\beta, \text{Enc}(), \text{Dec}()\}$ 。

询问阶段 1: $\mathcal{C}$ 构建一个初始列表 V 和一个集合 J , 列表最初是空的, $\mathcal{A}$ 进行以下询问。

私钥询问: $\mathcal{A}$ 对 $(\text{uid}, S_{\text{uid}})$ 进行私钥询问。 $\mathcal{B}$ 向 $\mathcal{C}$ 询问获得私钥, 随机选择 $t \in Z_p$, 并计算 RK :

$$\text{RK} = (K_0, \{K_{i,1}, K_{i,2}\}_{A_i \in S_{\text{uid}}}), \text{ 其中 } K_0 = H_1(\text{uid})^t, \text{ 对任意的 } A_i \in S_{\text{uid}}, K_{i,1} = g^{\alpha H_1(\text{uid})^{v_i t}}, K_{i,2} = H_1(A_i)^\beta.$$

$\mathcal{B}$ 将其发送给 $\mathcal{A}$, 维持列表 $D = D \cup \{S_{\text{uid}}\}$ 。

中间密钥询问: $\mathcal{B}$ 检查列表 V 中是否存在元组 $(S_{\text{uid}}, \text{RK}, \text{tpk})$ 。如果存在, 将其发送给 $\mathcal{A}$, 否则 $\mathcal{B}$ 随机选择 $d \in Z_p$, 计算密钥 $\text{tpk} = \{\text{tpk}_1 = K_{i,1}^d, \text{tpk}_2 = g^{\alpha d}, \text{tpk}_3 = K_0^d, A_i \in S_{\text{uid}}\}$, 并在表 V 中添加元组 $(S_{\text{uid}}, \text{RK}, \text{tpk})$ 。最后, $\mathcal{B}$ 将 tpk 发送给 $\mathcal{A}$ 。

挑战阶段: $\mathcal{A}$ 提供两条长度相等的挑战消息 k_0 和 k_1 。 $\mathcal{B}$ 选择 $b \in \{0, 1\}$ 以及访问结构 Γ^* 给 $\mathcal{C}$ 。 $\mathcal{C}$ 选择利用对称加密算法加密对称密钥得到密文 CT_b^* , 将其发送给 $\mathcal{B}$ 。 $\mathcal{B}$ 选择 $\vec{v} = \{s, v_2, \dots, v_n\}$, 并随机选择 $r_1, r_2, \dots, r_l \in Z_p^*$, 计算 $C = k_b \cdot e(g, g)^{\alpha s}$, $C_{1,i} = g^{r_i} g^{\lambda_i}$, $C_{2,i} = g^{r_i}$, $C_{3,i} = g^{v_{p(i)} r_i}$, $i \in [1, l]$, 并将 $\text{CT}_b = (C, \{C_{1,i}, C_{2,i}, C_{3,i}\}_{i \in [1, l]})$ 发送给 $\mathcal{A}$ 。

询问阶段 2: $\mathcal{A}$ 继续阶段 1 过程的查询, 只用于私钥询问的属性集不满足访问结构 Γ^* 。

猜测: $\mathcal{A}$ 输出猜测值 $b' \in \{0,1\}$ 。如果 $b = b'$, $\mathcal{B}$ 模拟了这个游戏。因此, 如果存在一个敌手 $\mathcal{A}$ 能以不可忽略的优势破解本文的方案, 那么也可构建一个挑战者以不可忽略的优势破解文献[25]的方案。

定理 2 本方案支持访问策略隐藏。

证明: 在本文方案中, 由 DO 部署访问策略来加密数据, 为了保护访问策略中的敏感信息, 通过哈希函数 H_1 使访问策略中的属性 att_i 盲化, 将访问策略中的属性信息 $A_i \in S_{\text{uid}}$, 计算 $q_i = e(H_1(\text{att}_i), g^\beta)$ 将属性替换, 实现访问策略的隐藏。

为了确保只有符合访问策略的用户才能访问和解密密文数据。访问者 DU 首先对任意的 $A_i \in S_{\text{uid}}$, 计算 $q' = e(g, K_{i,2})$ 并上传至区块链, 由区块链验证访问者的属性是否匹配, 即判断 $q'_i = q_i$ 是否成立。只有当等式成立时, 才能进行访问和解密操作。未经授权的攻击者从 $e(H_1(\text{att}_i), g^\beta)$ 无法获得关于访问策略的任何信息, 因此本方案实现了访问策略的隐藏, 保证了敏感信息的机密性。

6 性能分析

本文的电子病历共享方案, 支持细粒度的访问控制、策略隐藏、多关键字搜索以及云服务器外包解密。将本方案与相关方案的功能进行对比, 然后分析本方案的计算效率, 最后进行数值模拟实验评估。

6.1 功能比较

如表 1 所示, 将本方案的功能特性与文献[14,16-19] 中进行对比, 文献[14]不支持访问策略的隐藏, 存在患者隐私信息泄露的风险。本方案结合了区块链, 完成密文的安全搜索, 验证了访问者属性, 不需要数据访问者进行云上的验证, 减轻计算开销。文献[14]和文献[16]不能保证返回的密文的完整性。文献[14]和文献[19]不支持外包解密, 与本方案相比,

解密的计算开销较大。所以, 本文方案在整体功能上具有一定的优势。

表 1 功能特性比较

方案	支持策略 隐藏	支持多关键 词搜索	密文完整性 验证	支持外包 解密
文献[14]	不支持	支持	不支持	不支持
文献[16]	支持	支持	不支持	支持
文献[18]	支持	不支持	支持	支持
文献[19]	支持	支持	支持	不支持
本方案	支持	支持	支持	支持

6.2 性能比较

如表 2 所示, 本方案与其他方案在加密、陷门生成和搜索阶段的计算开销进行对比。 E 、 P 和 H 分别表示指数运算的时间、双线性对运算的时间和哈希运算的时间, 且 $P > E > H$ 。 $|T|$ 表示系统属性数量, $|L|$ 表示访问策略中属性数量, $|S|$ 表示用户属性个数, $|X|$ 表示关键字个数, $|N|$ 表示搜索关键字的个数。

在加密阶段, 文献[14]不支持访问策略隐藏, 所以计算量较小。本方案和文献[16,19]中的方案为了隐藏访问策略, 防止信息泄露, 保护患者隐私, 涉及指数和对运算, 计算开销较大。但本方案与文献[16-17,19]中的方案相比, 计算开销相对较小。在陷门生成阶段, 文献[16,19]中的指数运算随用户属性数量 $|S|$ 和搜索关键词数量 $|N|$ 增加而增加, 而本方案仅使用一次指数运算。在搜索阶段, 文献[14,16,19]中的方案随着用户属性 $|S|$ 和搜索关键词 $|N|$ 的增加, 在此阶段的计算量快速增加, 而本方案搜索阶段的计算量变化缓慢, 搜索时间较少。

表 3 中, 分别用 $|G_1|$ 、 $|G_2|$ 和 $|Z_p|$ 表示群 G_1 、群 G_2 和 Z_p 的长度。每个方案的通信开销随着属性个数和关键词数量的增加而增加, 但本方案的私钥大小和陷门大小与其他方案相比增长较小, 具有较低的通信开销

表 2 计算量比较

Table 2 Computation comparison

方案	加密	陷门生成	搜索	解密
文献[14]	$(2 L +2)E + (X +1)H$	$(2 S + N +5)E$	$(2 S +3+ N)P + (2 S +2)E$	$(L +3)E + L P$
文献[16]	$(2 L + X +4)E + (2 X + L)H + L P$	$(2 N + S)E + S P + (1+2 N)E$	$(N +1)P + N P$	$(L +5)E + 2P$
文献[17]	$(6 L +1)E + (L +1)P$	—	—	$(L +1)E + L P$
文献[19]	$(2 L + X +3)E + L H + L P$	$(2 S + N +2)E + N H + S P$	$(2 S + N +2)P + E$	$2P + L E$
本方案	$(3 L +2)E + X H + L P$	$E + (N + S)H + S P$	$2P + N E$	$(L +2)E$

表 3 存储量比较

Table 3 Storage comparison

方案	密文大小	私钥大小	陷门大小
文献[14]	$(2 L +2+ X) G_1 + G_2 $	$(2 S +4) G_1 $	$(S +3) G_1 + S G_2 + N Z_p $
文献[16]	$(3 L +3+ X) G_1 + L G_2 $	$(2 S +3) G_1 $	$(2 S + L +1) G_1 + S G_2 + Z_p $
文献[17]	$(5 L +2) G_1 +(L +1) G_2 $	$(S +1) G_1 +2 S G_2 $	—
文献[19]	$(2 L +3+ X) G_1 + L G_2 $	$(S +1) Z_p +(2 S +1) G_1 $	$(2 S +3) G_1 + S G_2 + Z_p $
本方案	$(3 L +2) G_1 + G_2 $	$(2 S +1) G_1 $	$(N +2) G_1 + G_2 + N Z_p $

6.3 数值实验比较

本文的数值实验是在 Linux 操作系统下利用双线性对 PBC(Paring Based Cryptography)实现的, 使用 C 语言对算法进行编程, 在 PC 机(联想 R720, 8GB RAM, 2.50GHz CPU)的虚拟机环境中运行。如图 2-6 所示。

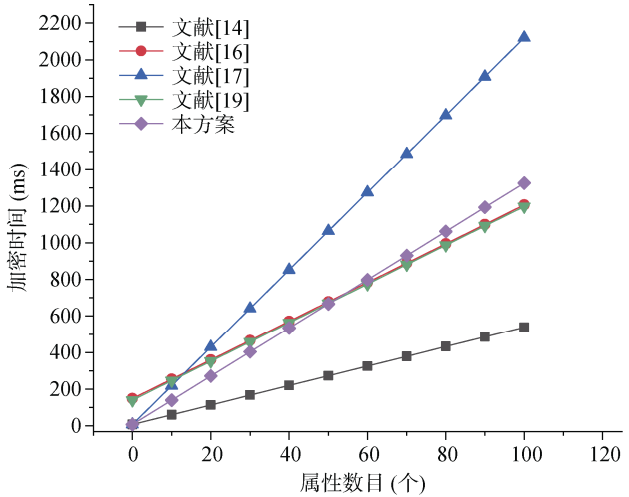


图 2 加密时间
Figure 2 Encryption time

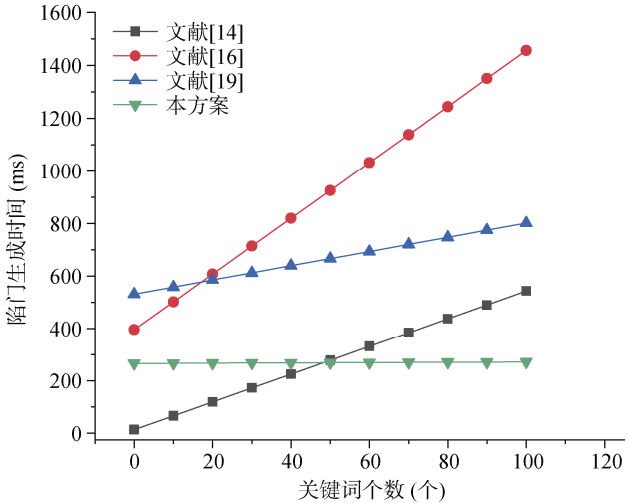


图 3 陷门生成时间
Figure 3 TrapGen time

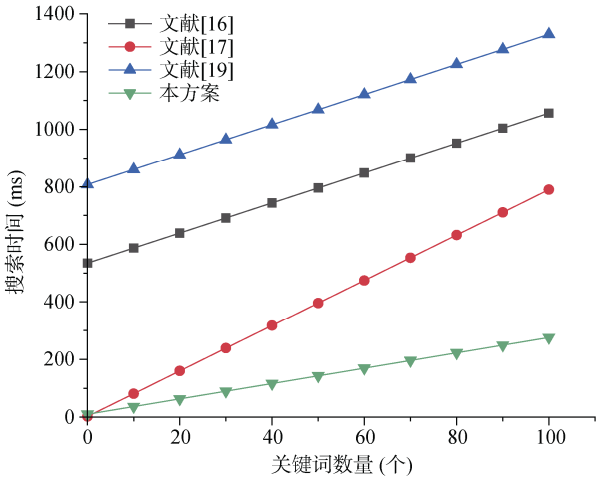


图 4 搜索时间(属性个数固定为 50 时)
Figure 4 Search time(Fixed number of attributes is 50)

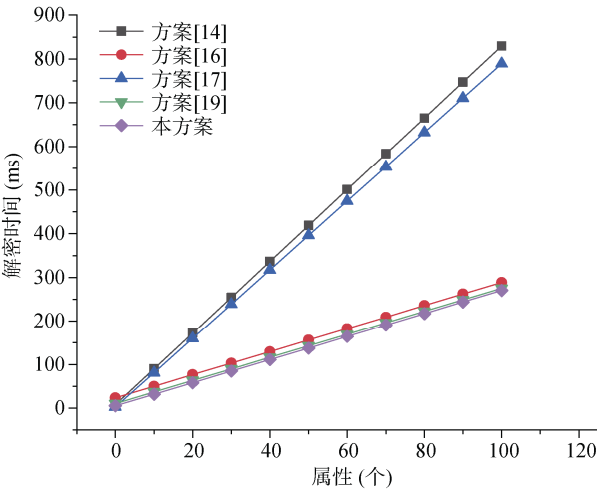


图 5 解密时间
Figure 5 Decrypt time

由图 2 可知, 当 $|L| < 70$, 本方案在加密阶段的计算开销小于文献[16-17,19]中的方案, 当 $|L| > 70$ 时, 本方案的计算开销略高于文献[16,19]中的方案。在加密阶段, 文献[14]不支持访问策略隐藏, 所以计算量较小。

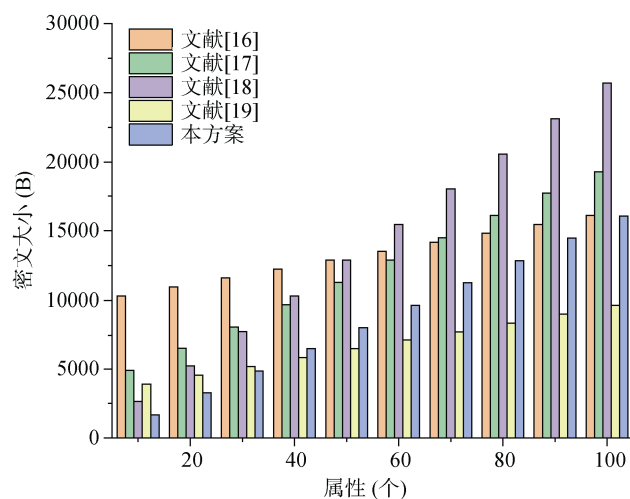


图 6 密文大小

Figure 6 The size of ciphertext

由图 3 可知, 随着用户属性和搜索关键词数量增加, 在陷门生成阶段, 本方案的时间小于文献[14,16,19]中方案的所需时间。

图 4 为当用户属性数量 $|S|=50$ 时, 搜索算法的时间开销, 由图 4 可知, 随着搜索关键词数量 $|N|$ 的增加, 本方案与文献[14,16,19]方案的时间开销都随着 $|N|$ 的增加而增加。而本文方案的增长速度是最低的, 明显低于其他方案。

本方案支持云服务器外包解密并优化了用户的解密效率, 由图 5 所示, 本方案的解密开销明显较小。相对于文献[16-17,19]解密的时间, 本方案优化了解密过程, 缩短了解密时间。

通信开销的对比如图 6 所示, 因为文献[14]不支持访问策略隐藏, 故通信开销小于文献[16,17,19]和本文方案。文献[17]的方案通信开销会随着属性数量的增加快速增加, 而本方案的密文大小增幅较缓慢, 通信开销较低, 减小了存储负担。

7 结论

本文提出了一种云环境下区块链辅助的属性加密电子病历方案。本方案利用属性基加密技术实现更细粒度的访问控制, 同时基于多关键字可搜索的加密技术, 完成关键字在区块链上的搜索工作, 保证数据密文的正确性。此外通过外包计算机制, 大大降低了数据访问用户的计算负担。最后安全性分析和性能分析表明, 本方案保证了安全性的同时, 实现了方案的有效运行, 因此在电子病历的数据共享场景下, 具有一定的实用价值。在未来的工作中, 将继续深入研究, 提高算法效率。

参考文献

- [1] Singh A P, Pradhan N R, Luhach A K, et al. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications[J]. *IEEE Transactions on Industrial Informatics*, 2021, 17(8): 5779-5789.
- [2] Song D X, Wagner D, Perrig A, et al. Practical techniques for searches on encrypted data[C]. *Proceeding 2000 IEEE Symposium on Security and Privacy*, 2002: 44-55.
- [3] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public Key Encryption with Keyword Search[M]. *Advances in Cryptology - EUROCRYPT 2004*. Berlin, Heidelberg: Springer, 2004: 506-522.
- [4] Fan Y Q, Liu Z H. Verifiable Attribute-Based Multi-Keyword Search over Encrypted Cloud Data in Multi-Owner Setting[C]. *2017 IEEE Second International Conference on Data Science in Cyberspace*, 2017. DOI:10.1109/dsc.2017.36.
- [5] Babu T K, Guruprakash C D. Multi-Keyword Text Search with Merkle Hash Tree for Privacy Preservation over the Encrypted Data[C]. *2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques*, 2019. DOI:10.1109/iceccot46775.2019.9114705.
- [6] Sun W H, Wang B, Cao N, et al. Verifiable Privacy-Preserving Multi-Keyword Text Search in the Cloud Supporting Similarity-Based Ranking[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2014, 25(11): 3025-3035.
- [7] Sahai A, Waters B. Fuzzy Identity-Based Encryption[C]. *Advances in Cryptology*, 2005: 457-473.
- [8] Li R H, Zheng D, Zhang Y H, et al. Attribute-Based Encryption with Multi-Keyword Search[C]. *2017 IEEE Second International Conference on Data Science in Cyberspace*, 2017. DOI:10.1109/dsc.2017.97.
- [9] Yin X C, Wang M Y, Ning J T. Lightweight searchable medical data sharing scheme[J]. *Journal on Communications*, 2022, 43(5): 110-122.
(殷新春, 王梦宇, 宁建廷. 轻量级可搜索医疗数据共享方案[J]. *通信学报*, 2022, 43(5): 13.)
- [10] Miao Y B, Ma J F, Liu X M, et al. M2-ABKS: Attribute-Based Multi-Keyword Search over Encrypted Personal Health Records in Multi-Owner Setting[J]. *Journal of Medical Systems*, 2016, 40(11): 246.
- [11] Wang J W, Ning J T, Xu S M, et al. Searchable attribute-based encryption scheme for dynamic user groups[J]. *Journal of Software*, 2023, 34(4): 1907-1925.
(王经纬, 宁建廷, 许胜民, 等. 面向可变用户群体的可搜索属性基加密方案[J]. *软件学报*, 2023, 34(4): 1907-1925.)
- [12] Yang G, Guo R, Zhuang C Y, et al. Dynamically updatable attribute based proxy re-encryption scheme in cloud[J]. *Journal of Cyber Security*, 2022, 7(3): 43-55.
(杨耿, 郭瑞, 庄朝源, 等. 云中可动态更新的属性基代理重加密方案[J]. *信息安全学报*, 2022(003): 007.)
- [13] Xu C, Wang N N, Zhu L H, et al. Achieving Searchable and Privacy-Preserving Data Sharing for Cloud-Assisted E-Healthcare System[J]. *IEEE Internet of Things Journal*, 2019, 6(5): 8345-8356.
- [14] Miao Y B, Ma J F, Liu X M, et al. Attribute-Based Keyword Search over Hierarchical Data in Cloud Computing[J]. *IEEE*

Transactions on Services Computing, 2017: 1.

- [15] Li S S, Xu C X, Zhang Y, et al. Efficient Data Retrieval over Encrypted Attribute-Value Type Databases in Cloud-Assisted Ehealth Systems[J]. *IEEE Systems Journal*, 2022, 16(2): 3096-3107.
- [16] Liu X Y, Lu T T, He X M, et al. Verifiable Attribute-Based Keyword Search over Encrypted Cloud Data Supporting Data Deduplication[J]. *IEEE Access*, 2020, 8: 52062-52074.
- [17] Belguith S, Kaaniche N, Laurent M, et al. PHOABE: Securely Outsourcing Multi-Authority Attribute Based Encryption with Policy Hidden for Cloud Assisted IoT[J]. *Computer Networks*, 2018, 133: 141-156.
- [18] Yang X D, Liao Z F, Liu L, et al. Power data sharing scheme based on blockchain and attribute-based encryption[J]. *Power System Protection and Control*, 2023, 51(13): 169-176.
(杨小东, 廖泽帆, 刘磊, 等. 基于区块链和属性基加密的电力数据共享方案[J]. *电力系统保护与控制*, 2023, 51(13): 169-176.)
- [19] Niu S F, Song M, Fang L Z, et al. Keyword Search over Encrypted Cloud Data Based on Blockchain in Smart Medical Applications[J]. *Computer Communications*, 2022, 192: 33-47.
- [20] Liu S H, Yu J G, Xiao Y H, et al. BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT[J]. *IEEE Internet of Things Journal*, 2020, 7(9): 7851-7867.
- [21] Niu S F, Xie Y Y, Yang P P, et al. Cloud-Assisted Attribute-Based Searchable Encryption Scheme on Blockchain[J]. *Journal of Computer Research and Development*, 2021, 58(4): 811-821.
(牛淑芬, 谢亚亚, 杨平平, 等. 区块链上基于云辅助的属性基可搜索加密方案[J]. *计算机研究与发展*, 2021.)
- [22] Su J, Zhang L Y, Mu Y. BA-RMKABSE: Blockchain-Aided Ranked Multi-Keyword Attribute-Based Searchable Encryption with Hiding Policy for Smart Health System[J]. *Future Generation Computer Systems*, 2022, 132: 299-309.
- [23] Wang Z R, Zheng D, Guo R, et al. Block chain -Enabled Anonymous Searchable Encryption Scheme in the Group Communication[J]. *Journal of Cyber Security*, 2022, 7(3): 134-148.
(王泽锐, 郑东, 郭瑞, 等. 群组内基于区块链的匿名可搜索加密方案[J]. *信息安全学报*, 2022(003): 007.)
- [24] Niu S F, HAN S, Xie Y Y, et al. Attribute-based searchable encryption scheme supporting multiple keywords based on blockchain.[J]. *Journal of Cyber Security*, 2023, 8(01): 131-143.
(牛淑芬, 韩松, 谢亚亚, 王彩芬. 基于区块链的多关键字属性基可搜索加密方案[J]. *信息安全学报*, 2023, 8(01): 131-143.)
- [25] Waters B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization[C]. *Public Key Cryptography*, 2011: 53-70.



李亚红 博士, 兰州交通大学电子与信息工程学院副教授, 硕士生导师, 研究领域为密码学与信息安全。Email: 359107023@qq.com



李强 于 2021 年在兰州交通大学大学通信工程专业获得学士学位。现在兰州交通大学信息与通信工程专业攻读硕士学位。研究领域为密码学与信息安全。Email: 1477051542@qq.com



李哲玮 于 2021 年在兰州交通大学通信工程专业获得学士学位。现在兰州交通大学信息与通信工程专业攻读硕士学位。研究领域为密码学与信息安全。Email: 1743469137@qq.com



王彩芬 博士, 深圳技术大学大数据与互联网学院教授, 博士生导师, 主要研究方向为大数据安全。Email: wangcaif@sztu.edu.cn



杨小东 博士, 西北师范大学教授, 硕士生导师, 主要研究方向为现代密码学和云计算安全。Email: y20s0888@163.com