表 1 diabetic_data 数据集外部描述词汇

词汇	前缀	类型
title	dc	数据集标题
theme	dcat	所属主题
description	dc	描述说明
Identifier	dc	数据集的唯一标识
keyword	dcat	关键词
format	dc	数据集格式
accessURL	dcat	访问链接
byteSize	dcat	数据集大小
license	dc	许可说明
Rights	dc	使用权限信息
Issued	dc	初始发布时间
modified	dc	最后修改时间

表 2 diabetic_data 数据集内部描述词汇

词汇	类型	说明
account_name	string	节点账户
Copyrightowner	string	数据集所属人
Field	string	数据集类别
MD5	string	数据集哈希值


```
[Metadata of diabetic_dataset]
"account_name": "Bob",
"CopyrightOwner": "Bob",
"identifier": "diabetic_dataset",
"title": "Diabetes 130-US hospitals for years 1999-2008 Data Set",
"theme": "This data has been prepared to analyze factors related to
        readmission as well as other outcomes pertaining to
        patients with diabetes.",
"keyword": "Diabetes;1999-2008;Medical cases;US",
"issued": "October 18th,2018 Thursday 20:20:17 CST",
"modified": "December 15th,2018 Saturday 15:20:01 CST",
"accessURL:"127.0.0.1/medical/datasets/Diabetes+130-US+hospitals
          +for+years+1999-2008",
"format": "csv",
"byteSize": "19,161,930 bytes",
"description": "The dataset represents 10 years (1999-2008) of clinical
              care at 130 US hospitals and integrated delivery networks.
              It includes over 50 features representing patient and
              hospital outcomes.",
"rights": "Authorized Access",
"license": "MIT",
"field": "Medical",
"MD5": "f22425753cefbc18e321825450ec0f00"
```


图 3 diabetic_data 数据集元数据

4.2 实验结果及分析

4.2.1 运行时间分析

经实验测试, 两种方案的系统运行时间如图 4.

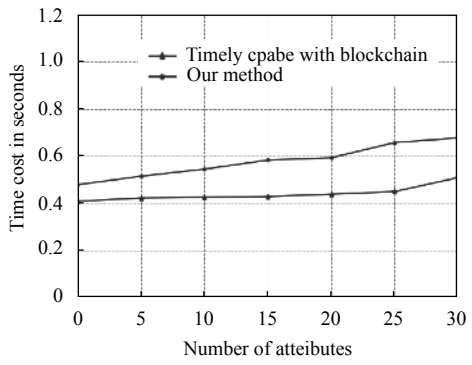

图 4 系统运行时间示意图

从图 4 可以看出, 随着属性数量的增加, 所需传输的密文和用户密钥的空间大小逐渐增大, 使得二者的系统运行时间逐步增加. 相对于 Timely CPABE with Blockchain 方案, DOB 框架的平均系统运行时间增加了 31.18%, 主要原因是采用序列化方法在链数据库上存储和传输密文、相关密钥和用户属性, 增加链数据库的读写次数. 但是, 系统运行时间远远小于 1 秒, 仍处于合理范围之内.

4.2.2 安全性分析

Timely CPABE with Blockchain 方案将合法请求者的用户属性公开存取在区块, 恶意节点可以盗用合法者的用户属性生成 *USK*, 从而将获得的密钥 k_2 与密钥 k_1 结合生成数据加密密钥 k. DOB 通过在链数据库上设置访问权限, 只有授权的数据请求者才能提取出密文、用户密钥 *USK* 和密钥 k_1, 因此 DOB 框架能降低 *USK* 被盗用的风险.

5 结论与展望

根据数据共享的安全需求, 本文提出一种基于 CP-ABE 和区块链的数据安全共享框架, 通过带有访问权限的智能合约部署密文—策略基于属性的加密, 提高了获取和跟踪共享数据访问许可的自动化程度, 使数据的管理使用权真正掌握在数据拥有者手中. 实验结果表明, DOB 框架的综合性能比 Jemel 等人提出的 Timely CPABE with Blockchain 方案表现得要好, 具有一定的积极意义. 由于访问策略是数据拥有者事先定义的, DOB 框架的访问机制相对固定, 适用于数据集自身更新频度小、共享范围相对确定的场景, 以避免数据加密的密钥频繁更换. 当然, 方案仍存在一些值得完善的地方, 例如属性灵活撤销、高效访问结构的设计以及访问策略动态更新, 以应用于动态共享场景, 将是下一步的研究方向.

参考文献

1 刘海房, 莫世鸿, 范冰冰. 开放数据最新进展及趋势. 情报杂志, 2016, 35(9): 163–167. [doi: 10.3969/j.issn.1002-1965.2016.09.029]

2 金泳, 徐雪松, 王刚, 等. 基于区块链的电子政务大数据安全共享研究. 信息安全研究, 2018, 4(11): 1029–1033. [doi: 10.3969/j.issn.2096-1057.2018.11.011]

3 Ahmadi Zeleti F, Ojo A, Curry E. Exploring the economic value of open government data. Government Information Quarterly, 2016, 33(3): 535–551. [doi: 10.1016/j.giq.2016.01.008]

4 中华人民共和国国务院. 促进大数据发展行动纲要. 成组技术与生产现代化, 2015, 32(3): 51–58. [doi: 10.3969/j.issn.1006-3269.2015.03.012]
5 冯登国, 张敏, 李昊. 大数据安全与隐私保护. 计算机学报, 2014, 37(1): 246–258.
6 戚学祥. 区块链技术在政府数据治理中的应用: 优势、挑战与对策. 北京理工大学学报 (社会科学版), 2018, 20(5): 105–111.
7 郭兵, 李强, 段旭良, 等. 个人数据银行——一种基于银行架构的个人大数据资产管理与增值服务的新模式. 计算机学报, 2017, 40(1): 126–143. [doi: 10.11897/SP.J.1016.2017.00126]
8 何蒲, 于戈, 张岩峰, 等. 区块链技术与应用前瞻综述. 计算机科学, 2017, 44(4): 1–7, 15. [doi: 10.11896/j.issn.1002-137X.2017.04.001]
9 Xu XW, Pautasso C, Zhu LM, *et al*. The blockchain as a software connector. Proceedings of 13th Working IEEE/IFIP Conference on Software Architecture. Venice, Italy. 2016. 182–191.
10 Di Francesco Maesa D, Mori P, Ricci L. Blockchain based access control. Proceedings of the 17th IFIP WG 6.1 International Conference, DAIS 2017, Held as Part of the 12th International Federated Conference on Distributed Computing Technique. Neuchâtel, Switzerland. 2017. 206–220.
11 Wang SP, Zhang YL, Zhang YL. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access, 2018, 6: 38437–38450. [doi: 10.1109/ACCESS.2018.2851611]
12 Jemel M, Serhrouchni A. Decentralized access control mechanism with temporal dimension based on blockchain. Proceedings of the IEEE 14th International Conference on E-business Engineering. Shanghai, China. 2017. 177–182.
13 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494.
14 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展. 软件学报, 2018, 29(7): 2092–2115. [doi: 10.13328/j.cnki.jos.005589]
15 Dannen C. Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. New York: Apress, 2017.
16 Clack CD, Bakshi VA, Braine L. Smart contract templates: Foundations, design landscape and research directions. arXiv preprint arXiv: 1608.00771, 2016.
17 Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina, Italy. 2011. 53–70.
18 苏金树, 曹丹, 王小峰, 等. 属性基加密机制. 软件学报, 2011, 22(6): 1299–1315.
19 Strack B, Deshazo JP, Gennings C, *et al*. Impact of HbA1c measurement on hospital readmission rates: Analysis of 70000 clinical database patient records. BioMed Research International, 2014: 781670.
20 于梦月, 翟军, 林岩. 我国地方政府开放数据的核心元数据研究. 情报杂志, 2016, 35(12): 98–104. [doi: 10.3969/j.issn.1002-1965.2016.12.018]