2024 年全国大学生信息安全竞赛

作品报告

作品名称：**PoliScope：安卓应用隐私政策与权限调用一致性的合规检测**

电子邮箱：**shenaowang@foxmail.com**

提交日期：**2024.05.24**

填写说明

1. 所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。

2. 作品报告采用 A4 纸撰写。除标题外，所有内容必需为宋体、小四号字、1.5 倍行距。

3. 作品报告中各项目说明文字部分仅供参考，作品报告书撰写完毕后，请删除所有说明文字。(本页不删除)

4. 作品报告模板里已经列的内容仅供参考，作者可以在此基础上增加内容或对文档结构进行微调。

5. 为保证网评的公平、公正，作品报告中应避免出现作者所在学校、院系和指导教师等泄露身份的信息。

目录

摘要

（请简要说明创作本作品之动机、功能、特性、创新处、实用性）

在当今数字化时代，随着信息技术的迅猛发展，患者就诊时医疗数据的产生和积累呈指数级增长，涵盖了个人诊疗状况、疾病诊断信息和基因组数据等，这些数据在就诊时的及时传递与共享对于患者的治疗决策、疾病确诊、临床治疗等方面具有重要意义。

然而，医疗数据的安全共享和利用同样面临着极大的挑战。一方面，现有的医疗机构存储的医疗数据往往仅在内部管理共享，彼此间并不相通，造成严重数据孤岛现象，使患者在进行跨机构就诊时需要准备多份电子病历；另一方面，医疗数据中包含患者的个人隐私敏感信息，在内部共享环境下仍存在部分医疗机构内部人员在未经患者同意的情况下使用这些数据，可能会导致患者隐私泄露；此外，医疗数据还具有一定的商业价值，如利用这些数据来定向投送医疗广告等，很容易成为不法分子恶意攻击进行牟利的对象。因此，在实现医疗数据多机构共享平台的同时，能够保障个人隐私安全具有重要的现实意义。

针对这些问题，基于分布式身份（Decentralized Identifiers，DID）技术实现医疗数据共享平台的想法应运而生。DID 技术基于区块链和分布式账本等技术，具有区块链透明、可追溯、不可篡改等优良特性，为每个参与者提供了独一无二的身份标识，实现了去中心化、安全、可验证的身份认证和授权管理。

通过基于 DID 技术的医疗数据共享平台，医疗数据的共享变得更加安全、高效和透明。医疗机构、医生、患者和研究人员可以在平台上自主管理和控制自己的数据，授权合适的权限给其他参与者，实现了医疗数据的可信共享和跨组织的协同合作。此外，基于智能合约的数据访问控制机制结合加密技术可以确保数据的安全性和隐私保护，有效解决了医疗数据共享中的信任和隐私问题。

在这样一个背景下，本文将设计与实现基于 DID 技术的医疗数据共享平台，分析其在促进医疗数据共享、优化医疗资源配置、保障隐私安全等方面的作用和价值，为医疗行业的数字化和个人隐私的安全保护提供支持。

（还会调整）

关键字： 1　2　3　4

Abstract

Keywords: Privacy Compliance NER Static Analysis Dynamic Analysis

第一章 作品概述

（建议包括：背景分析、相关工作、特色描述及应用前景分析等）

1.1 背景分析

在当今数字化时代，随着信息技术的迅猛发展，患者就诊时医疗数据的产生和积累呈指数级增长，涵盖了个人诊疗状况、疾病诊断信息和基因组数据等，这些数据在就诊时的及时传递与共享对于患者的治疗决策、疾病确诊、临床治疗等方面具有重要意义。

然而，医疗数据的安全共享和利用同样面临着极大的挑战。一方面，现有的医疗机构存储的医疗数据往往仅在内部管理共享，彼此间并不相通，造成严重数据孤岛现象，使患者在进行跨机构就诊时需要准备多份电子病历；另一方面，医疗数据中包含患者的个人隐私敏感信息，在内部共享环境下仍存在部分医疗机构内部人员在未经患者同意的情况下使用这些数据，可能会导致患者隐私泄露；此外，医疗数据还具有一定的商业价值，如利用这些数据来定向投送医疗广告等，很容易成为不法分子恶意攻击进行牟利的对象。可见，在实现医疗数据多机构共享平台的同时，如何保障个人隐私安全成为了医疗行业数字化的一大难题。

现有的医疗数据共享方式一般可分为两类：一种是集中式存储的医疗数据共享方式，另一种是分布式存储的医疗数据共享方式。前者使用广泛，但随时代发展暴露出如数据孤岛等诸多弊端；后者则则多以区块链技术为依托，以其分布式、匿名性、公开性和不可窜改的特点，在解决医疗信息共享问题上具有显著优势，但仍然具有 xxx、xxx 和 xxx 的弊端。因此，研究一种既能发挥分布式优势，又能减少/克服 xxx、xxx 的医疗数据共享方法具有重要的现实意义。

1.2 相关工作

1.2.1 Weidentity 区块链技术

1.2.2 分布式身份技术

1.3 特色描述

用户可以使用其 DID 作为身份标识，在不同医疗机构之间共享医疗数据，如病历、检查报告、影像数据等。用户可以通过授权方式，选择性地分享特定的数据给特定的医疗机构或医生，从而避免在不同医院之间重复进行相同的检查和检验。

通过数字身份（DID）技术，我们可以实现可靠的身份验证、精细的数据共享控制、隐私保护和便捷的健康管理，从而改善医患关系。患者可以更加信任地分享健康数据，医生可以更有效地提供个性化的医疗服务，促进医疗系统的协作和效率提升。用户选择性向医生揭秘一部分数据，医生能确保这些数据是来源正确可靠的，用户不能随意伪造数据，用户也能控制数据的披露程度

1.4 应用前景分析

第二章 作品设计与实现

（建议包括系统方案、实现原理、硬件框图、软件流程、功能、指标等）

表 **2.1**　一个简单的表格示例

实体标签	实体名称	实体举例	实体描述
CALENDAR	日历权限组	设备日历信息、读取日历	读/写/访问日历等权限
CAMERA	相机权限组	拍摄照片、访问摄像头	调用相机相关权限
CONTACTS	联系人权限组	查看通讯录、账户列表	读/写通讯录、账户列表等
LOCATION	位置权限组	定位服务、基站定位	获取粗略/精确位置等权限
MICROPHONE	麦克风权限组	录音，设备麦克风	访问麦克风及音频录制等权限
PHONE	手机状态权限组	IDFA、SIM 卡序列号	获取设备状态、通话记录等
SENSORS	传感器权限组	步数统计、运动与健康	访问设备传感器相关权限
SMS	短信权限组	短信授权、发送短信	读/写短信相关权限
STORAGE	存储权限组	访问相册、外部存储	读/写存储空间相关权限

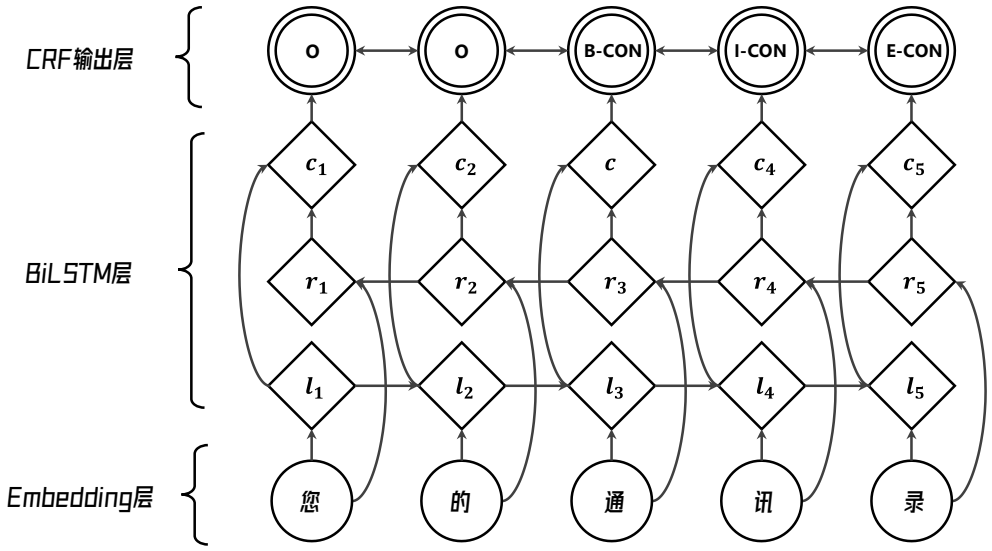

图 **2.1**　图片示例

第三章 作品测试与分析

（建议包括测试方案、测试环境搭建、测试设备、测试数据、结果分析等）

第四章 创新性说明

（本部分内容主要说明作品的创新性）

第五章 总结

参考文献

[1] 工业和信息化部. 互联网和相关服务业运行情况 [EB/OL]. [2022-04-29]. https://www.miit.gov.cn/gxsj/tjfx/hlw/index.html.

[2] 中国消费者协会. 100 款 App 个人信息收集与隐私政策测评报告 [EB/OL]. [2018-11-28]. https://cca.cn/jmxf/detail/28310.html.

[3] Arzt S, Rasthofer S, Fritz C, et al. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps[J]. Acm Sigplan Notices, 2014, 49(6): 259-269.