MediChain:基于区块链的 EHR 细粒度访问控制与共享系统

一.成果完成人及所在单位： 杨佳欣，计算机与信息工程学院 指导教师：陈金铃

二.成果简介：

以电子医疗病历为研究对象，我们提出了一种基于联盟链的医疗数据隐私保护和共享方案，旨在解决传统医疗电子健康档案中患者隐私以及数据安全共享的问题。将患者的医疗数据（EHR）对称加密后存储在医院本地或者云端数据库，同时将 EHR 敏感数据哈希操作之后和非敏感数据一起上传至区块链，区块链可将不同医疗机构的数据通过同一格式存储在链上，实现医疗数据跨平台、跨机构共享。基于密文策略的属性加密算法（ciphertextpolicy attribute-based encryption，CPABE）来确定具有符合访问控制结构的数据请求者才能够访问数据，同时，同态加密结合智能合约能够让数据请求者在不知道病人具体患病信息情况下实现对病人病情的盲化判断。

三. 主要研究内容及创新点：

在传统的患者就诊流程当中，所有病人信息都存放在医疗机构计算机系统中，涉及患者的隐私，中心化的数据存储模式易受到攻击导致未加密的患者隐私泄露，将患者隐私数据加密并哈希运算之后上传至区块链可以有效解决这种问题，患者可以授权数据拥有者共享权限，在其他医疗机构就诊时无需重复建立电子健康档案。同时，通过对 CP-ABE 算法的改进（见图 1），对于想要访问患者病情信息的医疗机构用户，必须符合患者设置的访问结构才能够访问，而且所获得的也不是患者的全部明文信息，而是哈希值和 AES 密钥，需要得到数据拥有者授权之后才能够访问全部信息。在病情诊断时，利用同态加密机制结合智能合约可以在不暴露患者病情的情况下对患者的体检情况进行诊断，从而有效保护患者隐私。

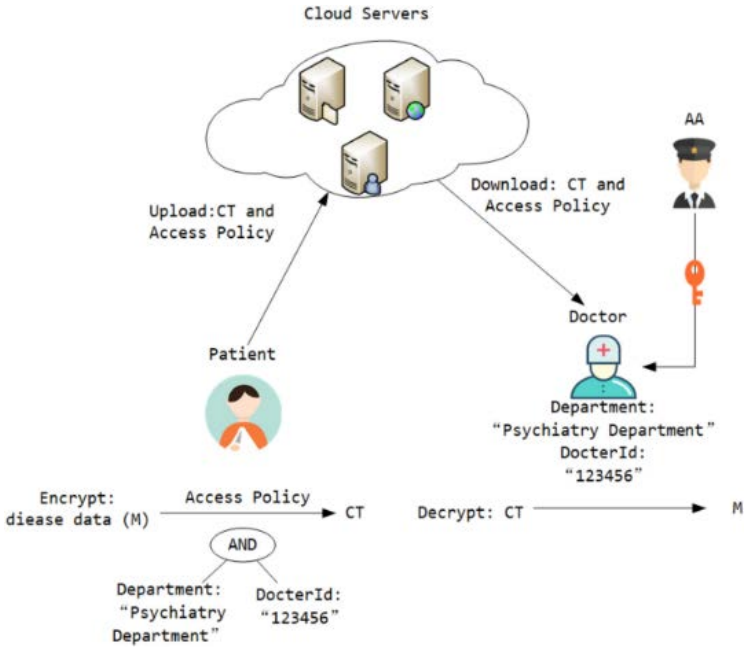


图 1 改进的 CP-ABE 算法流程图

四. 主要研究成果及应用情况

发表 SCI 论文与会议论文一篇。
授权实用新型专利一项。

联系人：杨佳欣 电 话：13002351091 Email:1045364021@qq.com