Proposal

**What are you trying to do?**

I am trying to implement a Medical Record system built in private blockchain, with Flask and python, that can stand challenging and concerning security and privacy.

**How is it done today? What are the limitations of the current practice?**

Nowadays, solutions are provided with features like consensus mechanisms like Proof of Stake and smart contract to dissolve issues. But limitations have been shown that consensus mechanism may consume energy, like electricity and/or time to compute results. As for smart contract, hackers have found and revealed vulnerabilities.

Blockchain 1.0 using consensus mechanism and Blockchain 2.0 using Smart contracts to implement security measures and prevent violation to privacy. However, real cases are occurring to unveil that such method does not fully ease the concerns for the purpose of protecting privacy and security.

**What is new in your approach and why do you think it can succeed?**

Homomorphic Encryption. The reason why I use such a encryption method is because Google has a similar project, but different in application scenarios and purpose, named Federated Learning which enables different institution or organization to share their data without compromising privacy or leak of data as their asset shared with others are protected by Homomorphic Encryption so that unrelated or unwanted parties/individuals will not be able to view and operate on the sensitive data.

In addition, I provide user-friendly interface to operate the system through web browser. The interface is simple and clean. The interface itself not only does not require users to climb sharp learning curve, but also the interface is implemented in a easy-to-maintain language Flask which can cooperate with SQLite database.

**Assuming you are successful, what difference does it make? To whom?**

To make it lightweight and friendly user-interface product for doctors so far. And mitigating the security and privacy problems by adopting the new features mentioned in the above question’s answer.

**How will you measure success? What are the “midterm and final exams”?**

I assume that I can perform visual hacker attack to simulate situations where common security and privacy problems occurred. The result and performance can be analyzed such that, for example, whether record is tempered or how long and many the attacks can sustain.

Introduction:

Utilize Blockchain and other method to enhance the security of medical files sharing and access. There has been increasing interest in connecting disjointed Electronic Medical Records, mobile health data, and related health data systems for the purpose of improving preventative and precision medicine, while also providing individuals with greater access and control to their data. Blockchains provide data transparency, immutability, and decentralized trust – making them a promising solution to the interoperability and security issues faced by such health data systems. Several papers have proposed the use of blockchain technology in healthcare to determine its viability as a solution and to identify potential applications and challenges.

Background

There are several security challenges and privacy concerns existing in the health/medical industry.

A screenshot of a cell phone

Description automatically generated

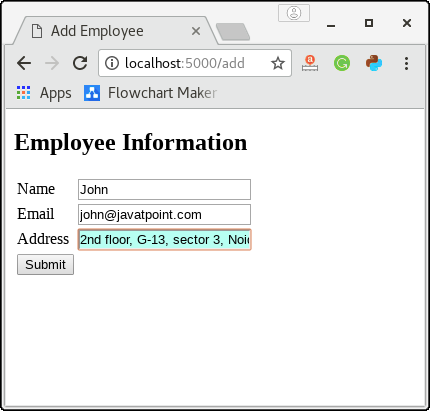
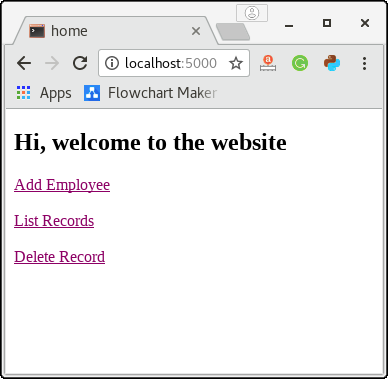
This table comes from “A survey on the security of blockchain systems” published in ELSEVIER’s Future Generation Computer Systems.

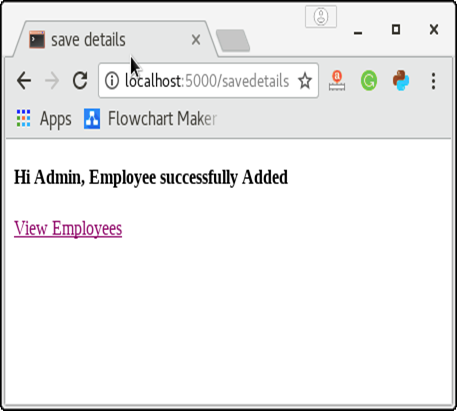
Plan:

The Blueprint of the system in general is the frontend is implemented in Flask and backend is implemented in python. Flask can work with SQLite to create a database where it stores a table contains user’s basic information and role. The backend is a private blockchain, implemented in python, where each block contains a record from a doctor, and doctor adds the block whenever the doctor needs. And each participant of the blockchain keeps a copy of the blockchain.

Data in each block from the block chain is protected by Homomorphic Encryption to guarantee the data owners’ rights. To operate on the related and intended data requires owners’ approval. The data can only be edited with such an approval. And such an operation is record in a log for the purpose of tracing with security needs.

The interface example:







提案

你想做什么？

我正在尝试使用Flask和python实施构建在私有区块链中的Medical Record系统，该系统可能具有挑战性并涉及安全性和隐私性。

今天怎么样？当前做法的局限性是什么？

如今，解决方案提供了诸如共识机制（如权益证明）和智能合约等功能来解决问题。但是已经显示出局限性，共识机制可能会消耗能量，例如电能和/或时间来计算结果。至于智能合约，黑客已经发现并揭示了漏洞。

使用共识机制的区块链1.0和使用智能合约的区块链2.0实施安全措施并防止侵犯隐私。但是，实际情况表明，这种方法不能完全缓解出于保护隐私和安全性的考虑。

您的方法中有什么新内容？为什么您认为它可以成功？

同态加密。之所以使用这种加密方法，是因为Google拥有一个类似的项目，但是在应用场景和目的上有所不同，名为Federated Learning，它使不同的机构或组织可以共享其数据，而不会损害与之共享的资产的隐私或数据泄漏。其他用户则受到同态加密的保护，因此无关或有害的团体/个人将无法查看和操作敏感数据。

另外，我提供了用户友好的界面，可以通过Web浏览器来操作系统。界面简单干净。该界面本身不仅不需要用户提高学习技巧，而且还以易于维护的语言Flask来实现，该语言可以与SQLite数据库配合使用。

假设你成功了，那有什么不同？给谁？

到目前为止，使其成为医生的轻巧友好的用户界面产品。并采用上述问题的答案中提到的新功能来缓解安全和隐私问题。

您将如何衡量成功？什么是“期中考试和期末考试”？

 我假设我可以执行视觉黑客攻击，以模拟发生常见安全和隐私问题的情况。可以对结果和性能进行分析，例如，对记录是否进行调节或攻击可以持续多长时间。

介绍：

利用区块链等方法增强医疗文件共享和访问的安全性。为了改进预防和精确医学，同时也为个人提供对其数据的更大访问和控制权，连接脱节的电子病历，移动健康数据和相关健康数据系统的兴趣日益浓厚。区块链可提供数据透明性，不变性和去中心化信任，这使它们成为解决此类健康数据系统所面临的互操作性和安全性问题的有前途的解决方案。几篇论文提出了在医疗保健中使用区块链技术来确定其可行性的解决方案，并确定潜在的应用和挑战。

背景

在健康/医疗行业中存在一些安全挑战和隐私问题。

该表来自ELSEVIER的Future Generation Computer Systems中发布的“关于区块链系统安全性的调查”。

计划：

系统的蓝图通常是在Flask中实现前端，在python中实现后端。 Flask可以与SQLite一起创建数据库，并在其中存储包含用户基本信息和角色的表。后端是一个用python实现的私有区块链，其中每个块都包含来自医生的记录，医生在需要时可以添加该块。区块链的每个参与者都保留一份区块链副本。

块链中每个块中的数据均受同态加密保护，以保证数据所有者的权利。要对相关数据和预期数据进行操作，需要所有者的批准。只能在获得批准的情况下编辑数据。并且出于跟踪安全需求的目的，将这样的操作记录在日志中。

接口示例：

**需求说明**

1、那我用多节点，需要中央服务器，中央服务器IP，端口确定，2，病例不可修改，但是可以追加修改到区块链，最后结果才是最终结果，中间数据相当于判定数据，3、医疗信息使用病人用户名进行加密，所有医生和相关病人能查看数据4、最后加密字段使用hash。

2、英文6000字左右 写清楚程序结构框图和数据结构

3、论文应用需要用英文