INSTITUTO DE INFORMÁTICA
Universidade Federal de Goiás

Software Design Document
Grupo 1

Projeto MedVault

INSTITUTO DE INFORMÁTICA
UFG

UFG
UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE INFORMÁTICA
Universidade Federal de Goiás

Contextualização, problema resolvido e objetivos

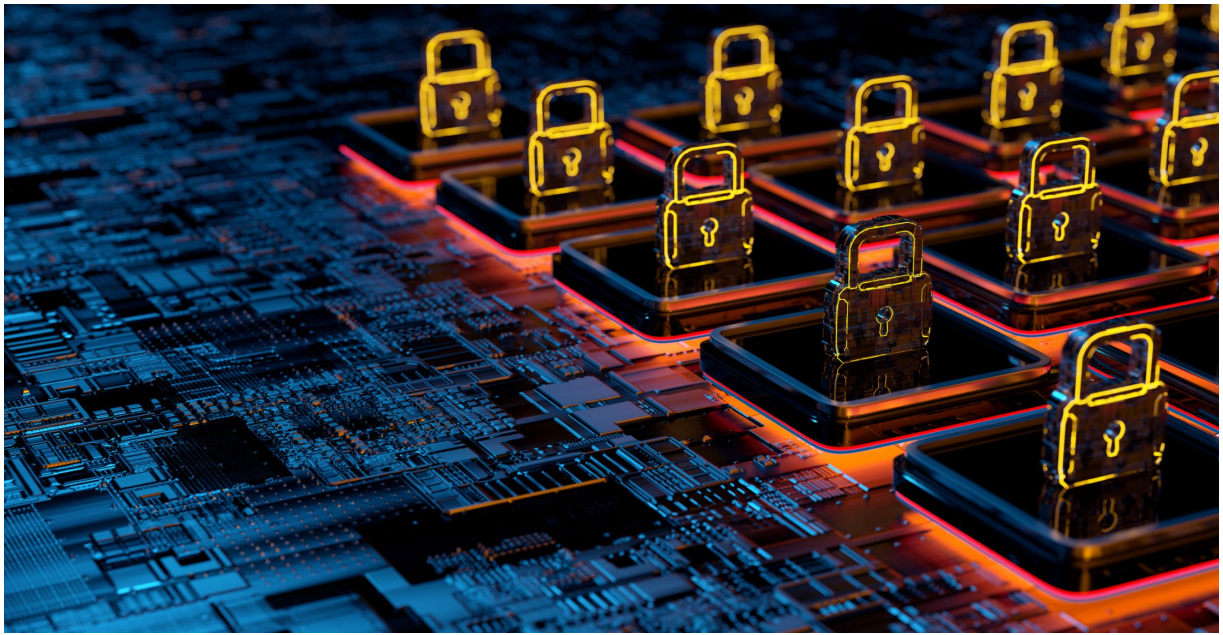
Contextualização

É de extrema importância nos atuais sistemas de saúde inteligentes a proteção dos dados confidenciais dos pacientes contra possíveis concorrentes/criminosos.

Assim, é vital ter mecanismos seguros de acesso aos dados que garantam que apenas entidades autorizadas possam acessar suas informações médicas, dada a devida autorização do cliente.

Problema resolvidos

Nosso projeto envolve, como forma de solução para o problema descrito, estudar e desenvolver um proxy de re-encriptação para a distribuição de documentos médicos ligados ao armazenamento offchain acoplado a um sistema blockchain.



Objetivos

- Desenvolver uma aplicação para armazenamento seguro e descentralizado de registros médicos usando Blockchain e IPFS.
- Desenvolvimento do proxy de reencriptação.
- Desenvolvimento de contratos inteligentes para blockchain.
- Desenvolvimento do módulo de armazenamento off-chain.

INSTITUTO DE INFORMÁTICA
Universidade Federal de Goiás

Requisitos de usuários e requisitos funcionais

Requisitos de usuários

- ***Registro de paciente***: O sistema deve permitir o registro de novos pacientes, coletando informações como nome, data de nascimento, gênero, endereço e outras informações relevantes para a identificação do paciente.

- ***Registro de histórico médico***: O sistema deve permitir que os médicos registrem o histórico médico de um paciente, incluindo diagnósticos, tratamentos anteriores, alergias, cirurgias realizadas, medicamentos prescritos e outras informações médicas relevantes.

- ***Compartilhamento controlado de informações***: O sistema deve permitir que os pacientes compartilhem suas informações médicas com outros profissionais de saúde ou instituições de forma controlada, ou seja, o paciente deve ter a capacidade de definir quais informações podem ser compartilhadas e com quem.

Requisitos funcionais

- ***Armazenamento descentralizado***: O sistema deve utilizar a blockchain para armazenar os registros médicos de forma descentralizada, garantindo a imutabilidade e a segurança dos dados. Além disso, os arquivos médicos devem ser armazenados no IPFS (distribuídos em uma rede peer-to-peer e identificados por meio de um hash criptográfico), que oferece um sistema de armazenamento distribuído e resiliente.

- ***Registro/Auditoria de transações***: Todas as transações envolvendo o histórico médico devem ser registradas na blockchain, incluindo a criação, modificação e compartilhamento de registros. Isso garante a transparência e a rastreabilidade das ações realizadas no sistema.

- ***Criptografia de dados:*** Os registros médicos e os arquivos anexados devem ser criptografados para garantir a confidencialidade e a segurança das informações armazenadas. Isso impede o acesso não autorizado aos dados, mesmo que eles sejam armazenados em uma rede descentralizada.

INSTITUTO DE INFORMÁTICA
Universidade Federal de Goiás

Fundamentos de SD relacionados

Descrição dos princípios de SD

- ***Transparência***: Um SD deve oferecer aos usuários e aplicativos a ilusão de que estão lidando com um único sistema de computação, em vez de várias máquinas separadas. No nosso caso, o usuário e os médicos possuem a impressão de que estão apenas se comunicando com um servidor qualquer, enquanto na verdade estão fazendo requisições para ler/modificar blocos específicos armazenados em uma blockchain descentralizada.

- ***Segurança***: A segurança dos dados e recursos em um sistema distribuído é um princípio fundamental. Mecanismos de autenticação, autorização e criptografia que serão implementados através do Hyperledger irão garantir a segurança dos dados.

- ***Escalabilidade:*** A capacidade de um sistema distribuído de lidar com um aumento na carga de trabalho ou no número de usuários é essencial. O Hyperledger Fabric utiliza uma arquitetura modular que permite a criação de canais privados e a divisão do processamento de transações entre diferentes nós da rede. Esse “sharding” pode aumentar a capacidade de processamento da rede, permitindo a execução simultânea de transações em diferentes partes da blockchain, trazendo uma maior escalabilidade para o sistema.

- ***Consistência:*** Em SDs, onde os dados são replicados e podem ser acessados por várias entidades concorrentes, é importante garantir a consistência dos dados. Em nosso caso, temos o IPFS usando o hash dos arquivos para verificar a integridade e garantir que eles não tenham sido corrompidos ou modificados (já que possuem um hash diferente para cada alteração), além dos algoritmos de consenso do Hyperledger que garantem que todos os nós concordem com a ordem e a validade das transações

Fundamentos de arquiteturas de SD e dos estilos arquiteturais

- ***Peer-to-peer (P2P)***

  Temos, por exemplo, que no IPFS os arquivos são divididos em blocos, distribuídos em uma rede peer-to-peer e identificados por meio de um hash criptográfico.

- ***Blockchain***

  Os registros do paciente estarão armazenados em diferentes blocos de uma blockchain descentralizada.

Descrição dos fundamentos de paradigmas de comunicação em SD

Comunicação baseada em troca de mensagens: Nesse paradigma, os componentes de um sistema distribuído se comunicam trocando mensagens. Cada componente pode enviar uma mensagem para outro componente, que então pode processar a mensagem e responder com uma mensagem de volta. Esse paradigma é geralmente implementado usando protocolos de comunicação, como o Transmission Control Protocol/Internet Protocol (TCP/IP) ou o User Datagram Protocol (UDP).

Robustez em sistemas distribuídos:

- ## Nomeação

O Hyperledger Sawtooth utiliza o conceito de endereços de recursos (Resource Addresses) para nomear entidades dentro do sistema. Esses endereços são gerados de maneira determinística a partir dos dados da transação, garantindo a unicidade e consistência dos identificadores. A nomeação adequada e a garantia de unicidade são importantes para evitar conflitos e assegurar a integridade dos dados.

- ## Coordenação

A coordenação em um sistema Hyperledger Sawtooth é facilitada pelo mecanismo de validação de transações distribuídas. Cada transação é submetida para validação em diferentes nós, e um algoritmo de consenso é usado para garantir que os nós cheguem a um acordo sobre a validade e a ordem das transações. Isso requer coordenação eficiente entre nós para sincronizar e validar as transações de forma consistente.

Robustez em sistemas distribuídos:

- ## Consenso

O Hyperledger Sawtooth utiliza um mecanismo de consenso modular, o que significa que diferentes algoritmos de consenso podem ser implementados e escolhidos de acordo com as necessidades do sistema. Algoritmos de consenso como o Proof of Elapsed Time (PoET) e o Practical Byzantine Fault Tolerance (PBFT) são comumente usados no Sawtooth para alcançar um consenso confiável e resistente a falhas, mesmo em ambientes distribuídos adversos.

- ## Consistência e replicação

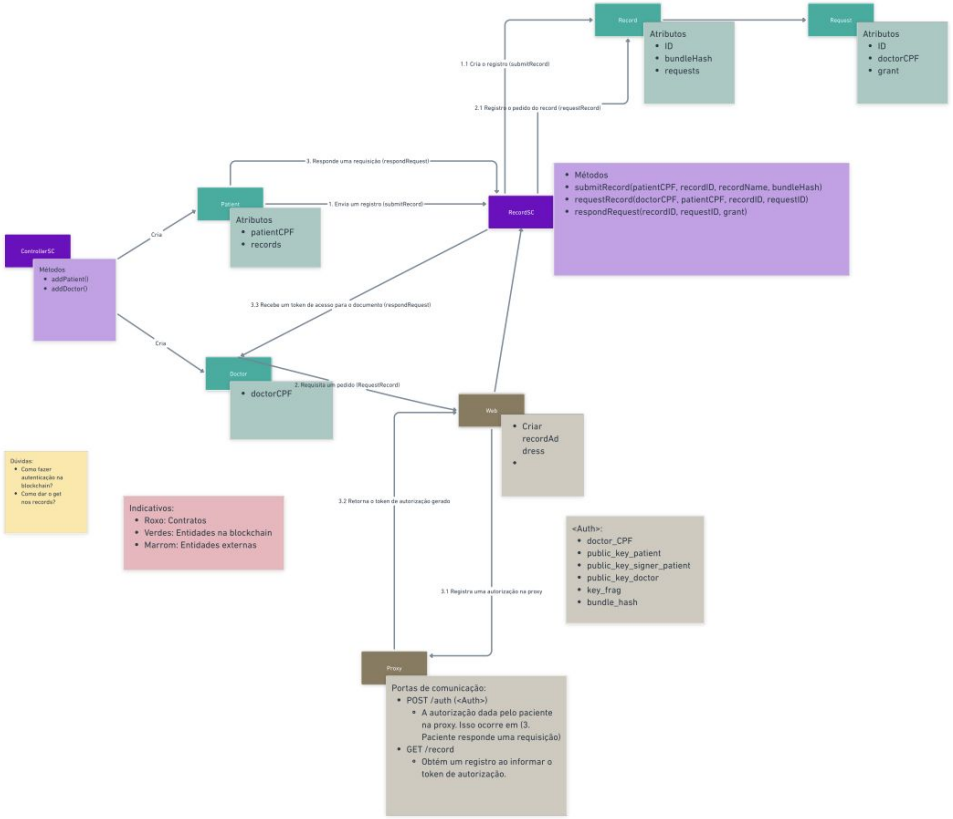
A consistência dos dados é garantida no Hyperledger Sawtooth por meio de um modelo de transações em estado de finalização (Transaction Family State). Cada transação atualiza o estado do blockchain de maneira atômica, garantindo que as operações ocorram de forma consistente e correta. Além disso, a replicação dos dados em vários nós aumenta a disponibilidade e a resistência a falhas do sistema, permitindo a continuidade do serviço mesmo quando alguns nós estão indisponíveis.

Robustez em sistemas distribuídos:

- **Tolerância**

  O Hyperledger Sawtooth é projetado para ser tolerante a falhas, tanto de nós quanto de redes. Os nós do Sawtooth possuem mecanismos de detecção de falhas e são capazes de se recuperar e se reconfigurar em caso de falhas. Além disso, o Sawtooth possui recursos para lidar com nós maliciosos ou desonestos, garantindo a segurança e a confiabilidade do sistema.

Design arquitetural



Referências

Referências Bibliográficas

Aplicação para armazenamento seguro e descentralizado de registros médicos usando Blockchain e IPFS

[1] ALATHUR, Sreejith; R., Swathy; ACHUTHAN, Krishnashree. A Blockchain-based System for Secure and Efficient Management of Medical Records. IEEE Access, v. 8, p. 23145-23156, 2020.

[2] CHAUDHARY, Shubham; MISHRA, Sanjay Kumar. Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. Computer Science Review, v. 39, p. 100307, 2021.

[3] PRASAD, Divya; PRASAD, Chandrika. Blockchain and IPFS-based Electronic Health Record System for Secure Sharing of Medical Data. International Journal of Engineering and Advanced Technology, v. 10, n. 2, p. 186-191, 2021.

Obrigado !