HealthID - Segurança da Informação

Introdução:

Ter informações pessoais na blockchain não é seguro por várias razões. A blockchain é projetada para ser imutável, o que significa que uma vez que os dados são gravados nela, eles não podem ser alterados ou apagados. Isso é uma característica fundamental para garantir a integridade dos registros. No entanto, se informações pessoais forem gravadas de forma irreversível, qualquer erro ou violação de privacidade não poderá ser corrigido.

Em vez de armazenar informações pessoais diretamente na blockchain, é mais seguro usá-la para gerenciar permissões de acesso e controlar o compartilhamento de dados pessoais armazenados de forma segura em sistemas externos, seguindo regulamentações de privacidade rigorosas. Isso ajuda a proteger a privacidade dos indivíduos enquanto aproveita os benefícios da tecnologia.

Em nosso projeto estamos lidando com informações médicas do usuário, então, precisamos tratar essas informações e garantir a privacidade do usuário, para somente depois disso inserirmos seus registros médicos na base de dados.

1. Identificação de Dados Sensíveis:

Na aplicação, o usuário vai carregar seu exame médico. Após ter sido feito o upload, o arquivo precisa ser convertido em texto e através de OCR (Optical Character Recognition) será feita a análise e busca das informações sensíveis (apenas os dados não sensíveis ou informações pseudonimizadas devem ser armazenados na blockchain). Informações pessoais que não sejam essenciais para o propósito da transação na blockchain (liberação de acesso aos dados médicos) serão removidas e armazenadas de forma centralizada e utilizando técnicas de anonimização.

2. Separação Física dos Dados:

Uma maneira de separar os dados é criando tipos de registros ou estruturas de dados distintos, exemplo: **registro de metadados,** este registro conterá informações de controle e metadados sobre o arquivo, como identificadores únicos, datas de criação, tipos de documentos e qualquer outra informação não sensível que seja útil e **registro de conteúdo,** este registro conterá o conteúdo real dos documentos, mas com os dados sensíveis anonimizados. Isso significa que as informações pessoais, como nomes e números de identificação, são substituídas por pseudônimos.

3. Referências Cruzadas:

Para garantir que o registro de metadados e o registro de conteúdo estejam relacionados, você pode usar um identificador exclusivo (como um código de hash ou ID) que vincule esses registros. Dessa forma, você pode recuperar os dados sensíveis quando necessário, mas apenas se a autorização apropriada for concedida.

4. Controle de Acesso:

Implementaremos um sistema de controle de acesso através de contratos inteligente para garantir que apenas partes autorizadas possam acessar os dados sensíveis. Isso permite que você defina permissões detalhadas sobre quem pode ver ou usar esses dados.

5. Auditoria e Rastreabilidade:

Registraremos todas as transações e atividades relacionadas ao acesso e uso dos dados, incluindo as autorizações concedidas e revogadas. Isso fornece rastreabilidade e histórico completo das interações com os dados sensíveis.

6. Conformidade com Regulamentações:

Todas as práticas de anonimização, pseudonimização e armazenamento de dados precisam estar em conformidade com as regulamentações de privacidade de dados, como o GDPR na União Europeia.

7. Educação do Usuário:

É necessário que os usuários sejam educados sobre como seus dados são protegidos e como eles podem controlar o acesso a essas informações, isso pode ser feito periodicamente.