Documentação do Protótipo de Detecção de Fraudes em Procedimentos Odontológicos

Introdução

Este documento descreve o funcionamento do protótipo de detecção de fraudes em procedimentos odontológicos. O sistema utiliza um modelo de aprendizado de máquina para analisar padrões de transações e identificar possíveis fraudes. Além disso, a API desenvolvida em Flask permite que outras aplicações consumam os serviços de previsão de forma prática e eficiente.

Objetivo do Projeto

O objetivo deste protótipo é fornecer uma camada adicional de segurança para clínicas odontológicas, ajudando na identificação de possíveis fraudes em transações e procedimentos. A partir de um conjunto de dados históricos, o modelo é treinado para reconhecer padrões suspeitos e sinalizar operações que podem representar riscos para a instituição.

Tecnologias Utilizadas

- **Linguagem de programação:** Python
- **Framework Web:** Flask
- **Bibliotecas de aprendizado de máquina:** Scikit-Learn
- **Modelo de aprendizado de máquina:** Random Forest
- **Banco de Dados Simulado:** Arquivo CSV
- **Interface Web:** HTML, CSS com Tailwind e JavaScript

Estrutura do Sistema

Treinamento do Modelo

Os dados históricos de transações odontológicas são carregados a partir de um arquivo CSV. O conjunto de dados é então dividido em dados de treinamento e teste. O modelo de aprendizado de máquina Random Forest é treinado com esses dados para identificar padrões associados a fraudes. Após o treinamento, o modelo é salvo para ser utilizado posteriormente na API.

API Flask para Previsão

A API expõe um endpoint que permite a análise de novas transações em tempo real. Quando um conjunto de dados de uma nova transação é enviado para o endpoint, o modelo realiza a análise e retorna um resultado indicando se a transação é segura ou suspeita. Esse retorno é fornecido no formato JSON, permitindo fácil integração com outras aplicações.

Como Usar a API

Executando o Servidor Flask

1. Instalar as dependências do projeto:
2. Executar o servidor Flask:
3. O servidor estará disponível no endereço `http://127.0.0.1:5000`

Realizando uma Requisição de Teste

Exemplo de Requisição

Exemplo de Resposta

A API recebe os dados da transação e utiliza o modelo treinado para determinar se a transação é suspeita ou não.

Interface Web

Além da API, foi desenvolvido um front-end para interação com o sistema. Esse front-end permite que os usuários insiram os dados da transação diretamente em um formulário e obtenham uma resposta sobre a detecção de fraude.

Possíveis Melhorias Futuras

- **Integração com banco de dados:** Atualmente, os dados são armazenados em arquivos CSV. Uma alternativa mais robusta seria a integração com um banco de dados relacional como OracleDB ou um banco NoSQL como MongoDB.
- **Dashboard de monitoramento:** Criar uma interface administrativa que permita acompanhar as previsões feitas pelo sistema e visualizar estatísticas sobre detecções de fraudes.
- **Autenticação e segurança:** Implementar autenticação de usuários para restringir o acesso à API e garantir que apenas usuários autorizados possam enviar transações para análise.
- **Retroalimentação:** Implementar a retroalimentação de dados de consultas para o sistema de aprendizado.

Conclusão

Este protótipo demonstra como o aprendizado de máquina pode ser aplicado para a detecção de fraudes em procedimentos odontológicos. A API desenvolvida permite que o modelo seja integrado a outras aplicações, proporcionando um mecanismo eficiente para a análise de transações suspeitas. O sistema pode ser expandido e aprimorado para atender a requisitos específicos de segurança e desempenho conforme necessário.

link do vídeo demonstrativo: https://youtu.be/1P7L7xhkrwQ