UNIFEOB

CENTRO UNIVERSITÁRIO DA FUNDAÇÃO DE ENSINO OCTÁVIO BASTOS

ESCOLA DE NEGÓCIOS

ANÁLISE E DENSENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO

"AI&SecTech”

MÓDULO INTELIGENCIA ARTIFICIAL

Inteligência Artificial – Prof. RODRIGO MARUDI DE OLIVEIRA

Projeto de Inteligência Artificial – Prof. RODRIGO MARUDI DE OLIVEIRA

Estudantes:

Erika Aparecida Cordeiro**, 1012023200127**

SÃO JOÃO DA BOA VISTA, SÃO PAULO

Novembro, 2023

RELATÓRIO DE DESENVOLVIMENTO DO PROJETO

1. Introdução:

O projeto consiste na implementação de um chatbot em Java, denominado PepeIT, que utiliza a API do OpenAI GPT-3. O chatbot visa fornecer uma interface interativa e amigável para os usuários, capaz de responder às suas consultas e proporcionar uma experiência de conversação natural. Além disso, são incorporadas medidas de segurança para proteger a interação do usuário.

2. Configuração Inicial:

O programa inicia com uma mensagem de boas-vindas e uma breve introdução ao chatbot. Esta estratégia visa criar uma interação acolhedora e informativa com o usuário, estabelecendo o propósito do chatbot. A palavra-chave 'exit' é disponibilizada para permitir que os usuários encerrem a conversa quando desejarem.

```
System.out.println("Bem-vindo! Meu nome é PepeIT, estou aqui para te auxiliar. Em que posso te ajudar hoje?  Digite 'exit' para sair.");
```

3. Lógica de Interação:

O chatbot opera em um loop contínuo, onde o usuário pode inserir suas consultas. O sistema aguarda a entrada do usuário, que é então enviada para a função `chatGPT` para interação com a API do GPT-3. A resposta gerada pelo modelo é exibida como a resposta do chatbot.

```
    String response = chatGPT(userInput);
    System.out.println("PepeIT: " + response);
}
```

4. Comunicação com a API do GPT-3:

A comunicação com a API do GPT-3 é implementada na função `chatGPT`. A função constrói a solicitação, envia-a para a API e processa a resposta, utilizando a chave de API fornecida. A resposta é então extraída e retornada para ser exibida ao usuário.

5. Manipulação da Resposta:

A função `extractContentFromResponse` é responsável por processar a resposta da API, extrair o conteúdo relevante (resposta gerada pelo GPT-3) e retorná-lo para ser exibida ao usuário.

6. Segurança do Usuário:

Para garantir a segurança do usuário, algumas medidas foram incorporadas:

Proteção da Chave de API: A chave de API é armazenada de forma segura, e medidas são adotadas para garantir que ela não seja exposta inadvertidamente. É recomendável considerar métodos de armazenamento criptografado e rotação periódica de chaves para evitar acessos não autorizados.

Filtragem de Entrada do Usuário: Antes de enviar a entrada do usuário para a API, pode-se implementar uma validação que filtre e sanitize a entrada, removendo caracteres maliciosos ou potencialmente perigosos. Isso ajuda a prevenir ataques de injeção de código.

Aviso de Informações Sensíveis: O chatbot pode ser projetado para reconhecer e não responder a solicitações que contenham informações sensíveis, como senhas, números de cartão de crédito, etc.

7. Conexão HTTP Segura:

A comunicação com a API do Openai GPT-3 é realizada por meio de uma conexão HTTP segura. O código utiliza a classe ‘HttpURLConnnection’ para configurar e enviar solicitações HTTP de forma segura, protegendo a integridade das comunicações.

```
try {
    URL obj = new URL(url);
    HttpURLConnection con = (HttpURLConnection) obj.openConnection();
    con.setRequestMethod(method:"POST");
```

8.Encerramento do Programa:

O programa oferece a opção de encerrar a interação quando o usuário digita 'exit'. Essa funcionalidade proporciona uma saída amigável e intuitiva para o usuário.

```
if (userInput.equalsIgnoreCase(anotherString:"exit")) {
    System.out.println(x:"Saindo do ChatGPT. Até mais!");
    break;
}
```

9. Considerações Finais:

Aprimoramentos Futuros: Além das medidas de segurança já implementadas, podem-se explorar aprimoramentos adicionais, como criptografia de comunicação, monitoramento de atividades suspeitas e políticas de privacidade claras para os usuários.

Este relatório abrange a implementação do chatbot em Java com a API do OpenAI GPT-3, destacando suas características principais, estrutura e medidas de segurança para proteger a interação do usuário. A segurança do usuário é uma prioridade crucial, e essas medidas ajudam a mitigar potenciais riscos associados à interação com o chatbot.

Abaixo, segue o link para a visualização do vídeo, onde é mostrado o ChatBot funcionando corretamente. A documentação, consiste em tópicos onde é explicado com detalhes de como a aplicação funciona na prática.

https://www.loom.com/share/4ea4d69ef6734ef29b6904227af5fbaa?sid=92023ad6-74b7-4baa-8770-a3731d0192ab

Link do GitHub, caso queriam analisar o código utilizado para esse projeto.

https://github.com/apserika/Chatbot.java.