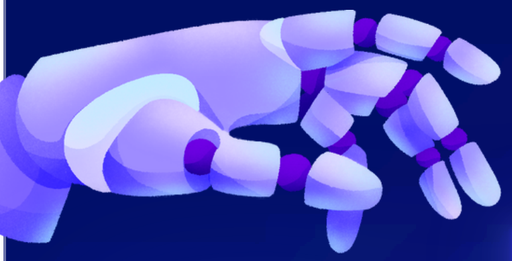
BSIDES VITÓRIA

DEVELOPERS VS AI

HOW TO DO SECURE CODE?

By Fabio Gomes ROcha



O QUE É IA GENERATIVA?

?

AONDE A IA GENERATIVA VEM SENDO USADA? OU É SÓ UMA MODA?

RAJBHOJ ET AL. 2024

E PORQUE ISSO IMPORTA?

Estudos mostram que desenvolvedores que usam ferramentas de IA generativa podem codificar até **55%** mais rápido

Lopes, 2023 (https://sapiensdev.com/blog/better-faster-stronger-software-developers-powered-by-generative-ai/)

IAs generativas como o ChatGPT podem aumentar a produtividade da força de trabalho em cerca de **14%.**

92% dos desenvolvedores dos EUA afirmam que usam ferramentas de IA como o ChatGPT para aumentar a produtividade em uma variedade de tarefas de programação.

Pesquisa do github

NEM TUDO SÃO FLORES

Do ponto de vista ético:

- uso apropriado da IA
- direitos autorais
- propriedade intelectual dos conteúdos gerados,
- bem como o potencial para criação de deepfakes

ChatGPT wrote code that can make databases leak sensitive information

Six AI tools, including OpenAI's ChatGPT, were exploited to write code capable of damaging commercial databases – although OpenAI appears to have now fixed the vulnerability

By Jeremy Hsu

25 October 2023

ChatGPT can leak training data, violate privacy, says Google's DeepMind

Simply instructing ChatGPT to repeat the word "poem" endlessly forced the program to cough up whole sections of text copied from its training data, breaking the program's guardrails.

Written by **Tiernan Ray,** Senior C

Dec. 4, 2023 at 2:05 a.m. PT

BREAKING

Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

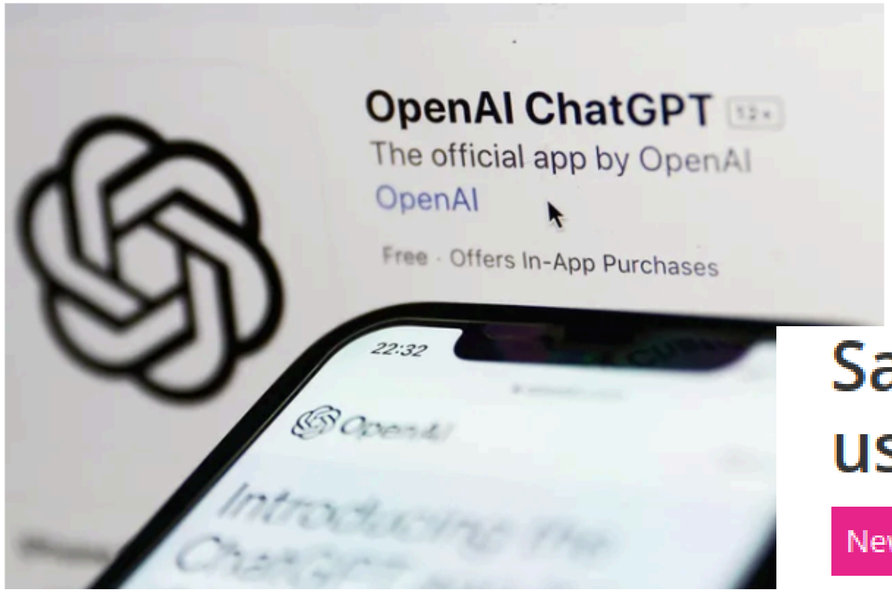
Siladitya Ray Forbes Staff

Siladitya Ray is a New Delhi-based Forbes news team reporter.

Follow

ARTIFICIAL INTELLIGENCE / TECH / APPLE

Apple restricts employees from using ChatGPT over fear of data leaks



/ Apple is the latest company to ban employees from using generative AI tools like ChatGPT. OpenAI's chatbot stores users' conversations to train the company's AI systems.

Samsung workers made a major error by using ChatGPT

News By Lewis Maddison published April 4, 2023

Samsung meeting notes and new source code are now in the wild after being leaked in ChatGPT

Google Bard Advanced leak hints at imminent launch for ChatGPT rival

News By Cesar Cadenas published January 5, 2024

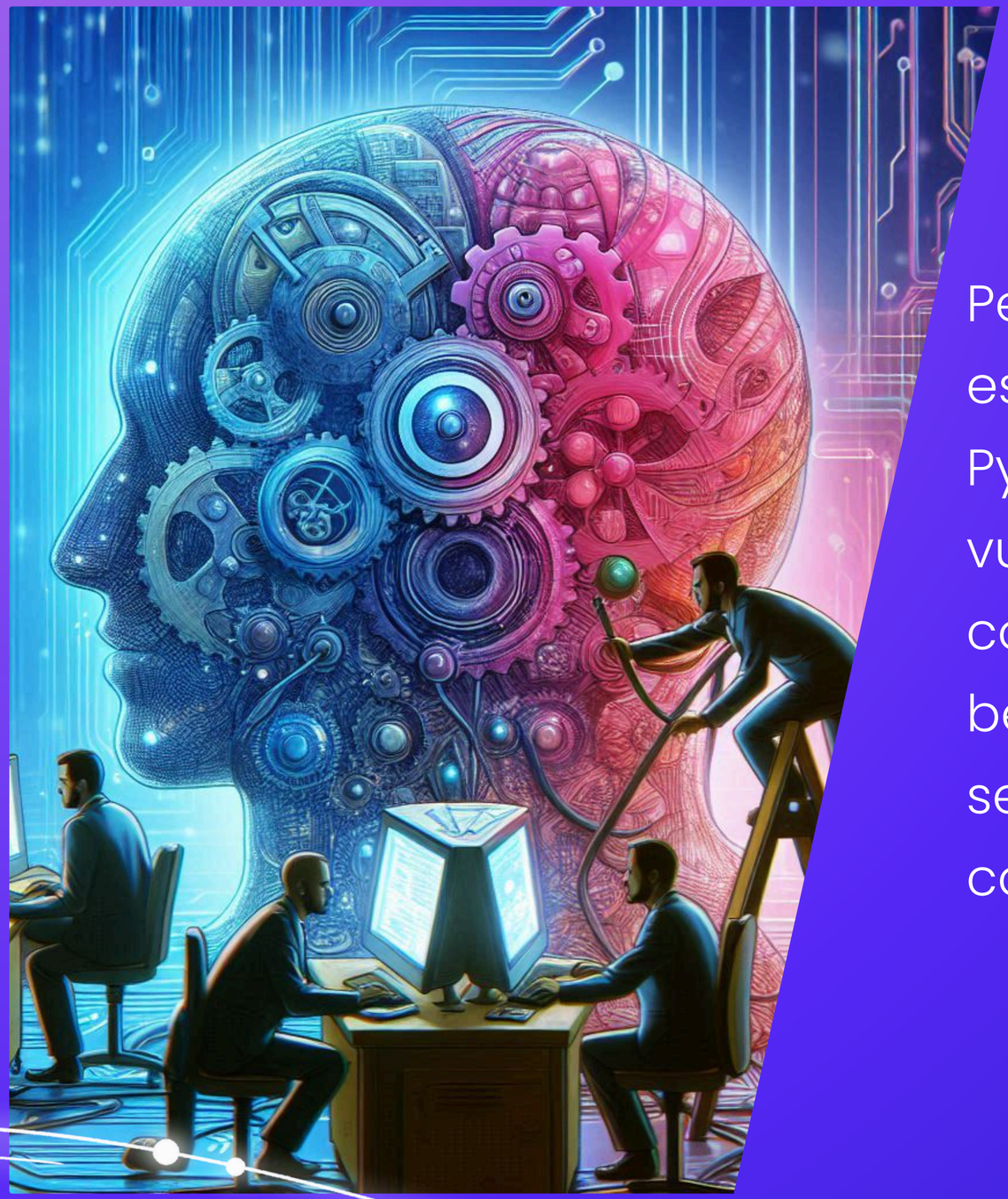
However, clues suggest it won't be free

Confiar no código produzido pelo ChatGPT significa potencialmente implantar código inseguro em um aplicativo de produção e introduzir vulnerabilidades sem querer. Isso é particularmente preocupante para usuários com pouco conhecimento prévio ou conhecimento incompleto desse domínio específico do código produzido por IA. Em um estudo de 2021, os pesquisadores descobriram que o CoPilot do GitHub – **produziu problemas de segurança em cerca de 40% das vezes.**

Trendmicro

Embora o ChatGPT possa gerar código funcional que atenda aos requisitos de um determinado prompt, ele geralmente produz código básico sem recursos básicos de segurança. Por exemplo, o código gerado pelo ChatGPT pode não ter validação de entrada, limitação de taxa ou até mesmo recursos básicos de segurança da API, como autenticação e autorização. Isso pode criar vulnerabilidades que os invasores podem explorar para extrair informações confidenciais do usuário ou executar ataques de negação de serviço (DoS).

Trendmicro



Pesquisadores do Canada realizaram um estudo, em 2023 com 4 linguagens C, C++, Python e Java e fizeram analise de vulnerabilidade, foi descoberto que o código gerado pela IA Generativa estava bem abaixo dos padrões mínimos de segurança, aplicáveis na maioria dos contextos.

RAJBHOJ ET AL. 2024

- Trate todo o código gerado pelo ChatGPT como se ele contivesse vulnerabilidades. Não assuma que é seguro porque uma IA altamente treinada gerou esse código.
- Complemente seu uso do ChatGPT com codificação manual. Não confie apenas no ChatGPT.
- Realize testes de segurança rigorosos em seus aplicativos.

- Faça com que o código seja revisado por colegas que possam detectar problemas de segurança.
- Consulte a documentação relevante, especialmente se você não estiver familiarizado com o idioma ou a biblioteca. Sempre faça sua pesquisa e não assuma que a IA sabe o que é melhor.

COMO REDUZIR PROBLEMAS?

SAST

DAST

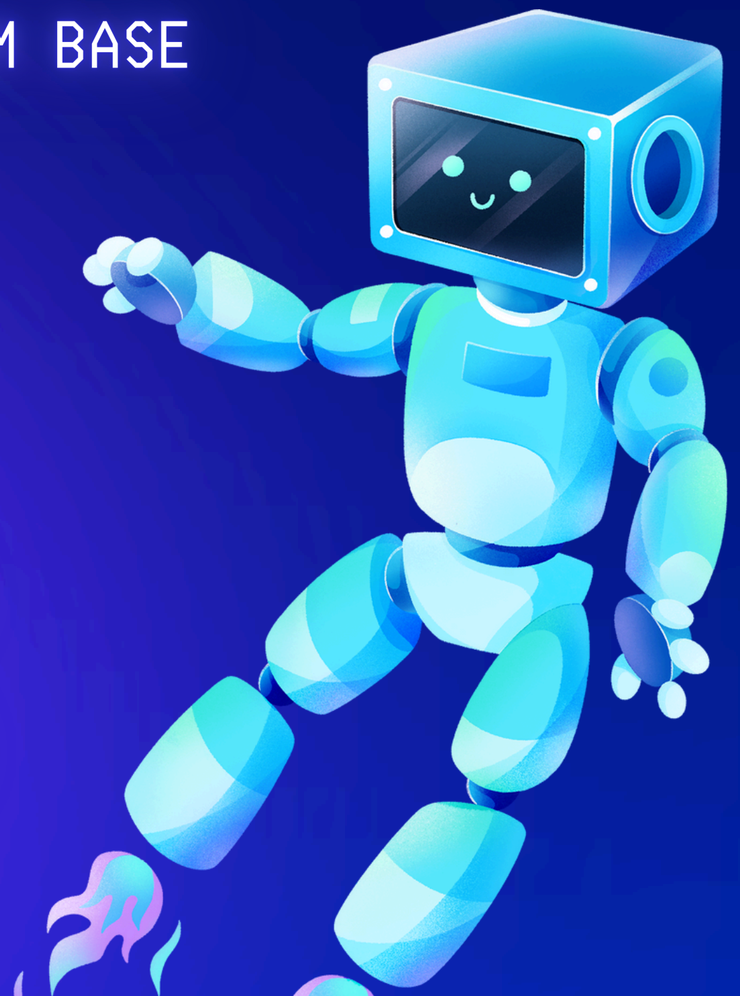
CODE REVIEW

SAIBA O QUE DESEJA DESENVOLVER

CRIE PROMPTS COM BASE EM REQUISITOS

ADOÇÃO DE IA GENERATIVA INTERNA

IA GENERATIVA COMO PARCEIRO, ESTILO PROGRAMAÇÃO EM PAR



COMO FAZER UM PROMPT EFETIVO?

01

Seja claro e específico

02

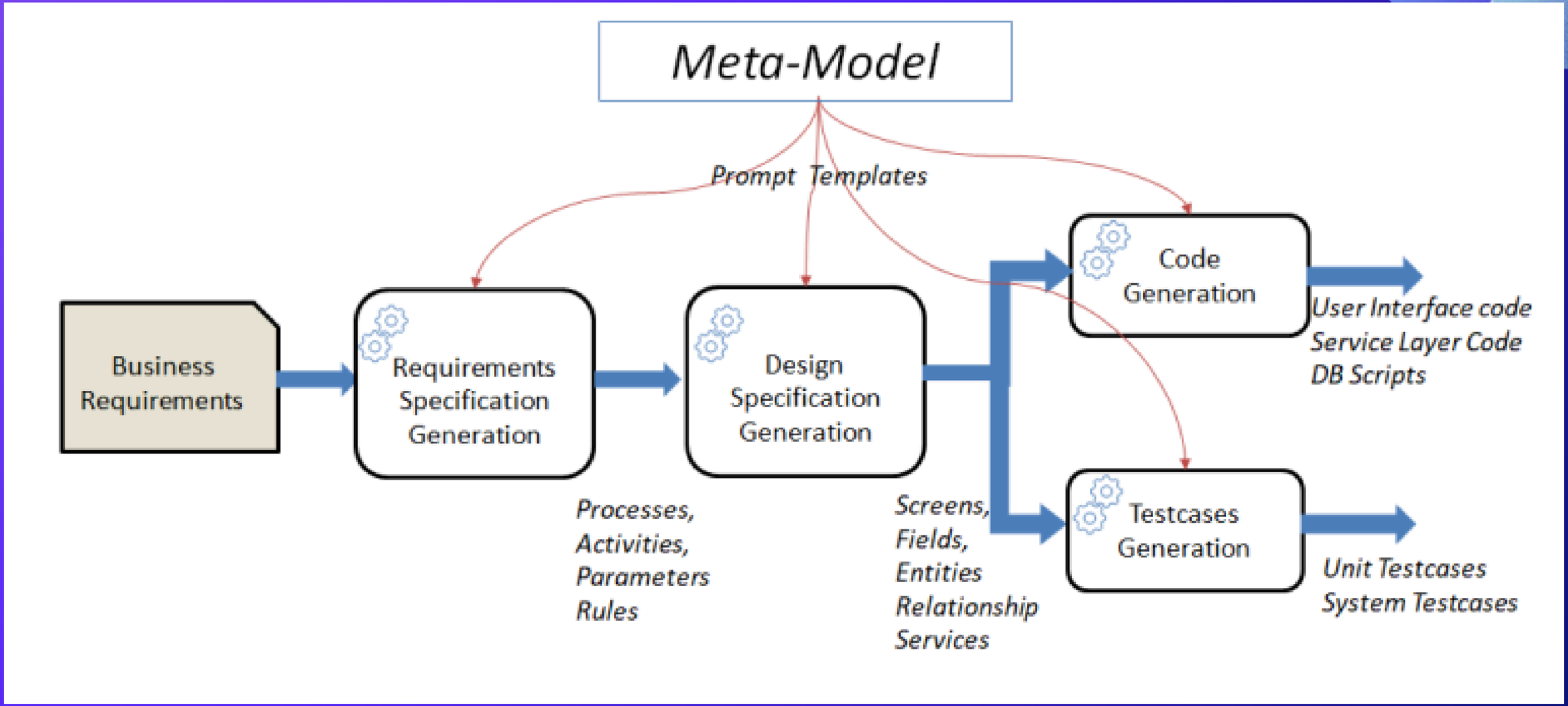
Explique o contexto

03

De exemplos

04

Permita a LLM lhe fazer perguntas


Meta-Model
Prompt Templates
Business Requirements
Requirements Specification Generation
Design Specification Generation
Code Generation
Testcases Generation
User Interface code
Service Layer Code
DB Scripts
Unit Testcases
System Testcases
Processes,
Activities,
Parameters
Rules
Screens,
Fields,
Entities
Relationship
Services

ESPECIFICAÇÃO DE REQUISITOS

INPUT: <BUSINESS DOMAIN>, <CONTEXT>, <BUSINESS REQUIREMENTS>

DESIGN DE SISTEMAS

INPUT: <BUSINESS DOMAIN>, <PROCESS SPEC:

REQUIREMENT SPEC

PROMPT 2 RESPONSE>, <RULES SPEC: REQUIREMENT

SPEC PROMPT 3

RESPONSE>

GERAÇÃO DE CÓDIGO

INPUT: <BUSINESS DOMAIN>, <TECHNOLOGY STACK>, <ER SPEC: DE-SIGN SPEC PROMPT 1 RESPONSE>, <SERVICES SPEC: DESIGN SPEC PROMPT 2 RESPONSE>, <SCREENS SPEC: DESIGN SPEC PROMPT 5 RESPONSE>

GERAÇÃO DE TESTES

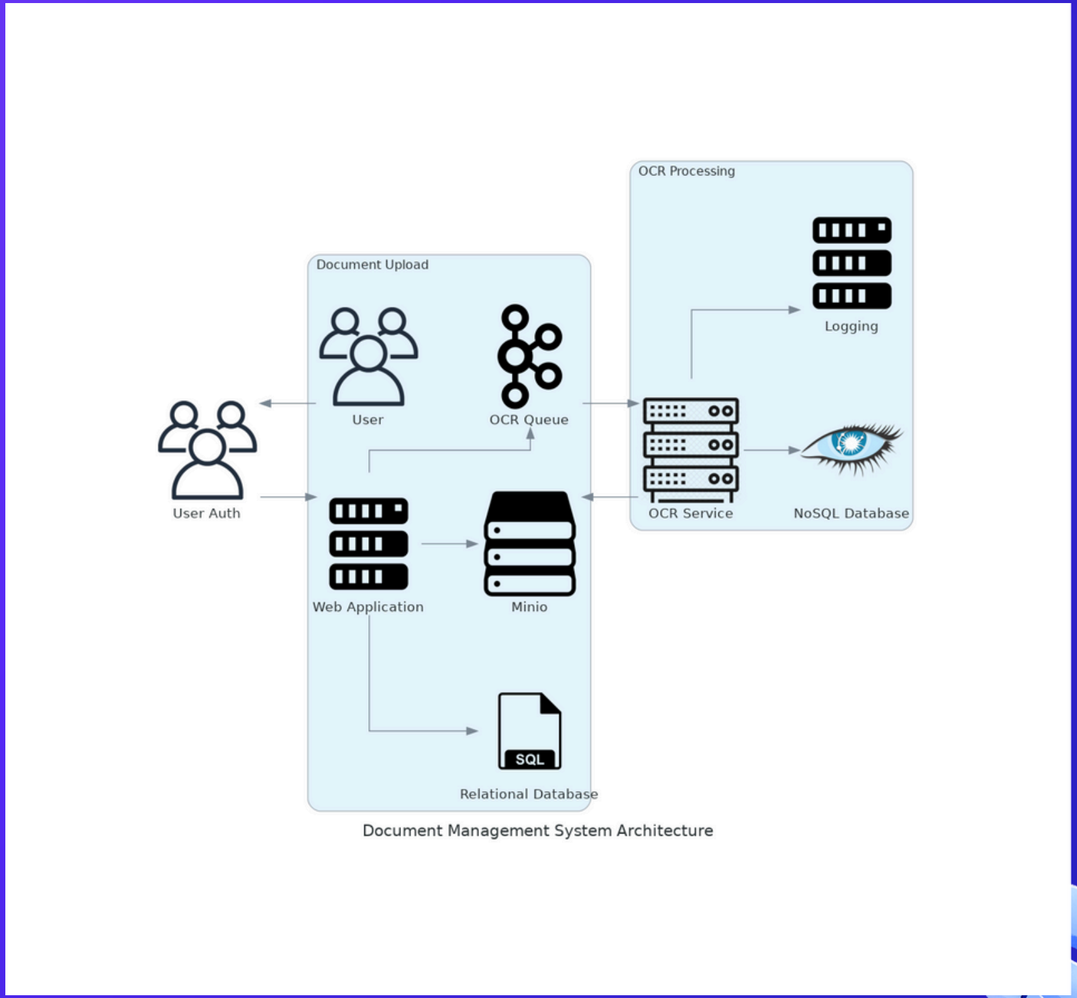
INPUT: <BUSINESS DOMAIN>, <SERVICES SPEC: DESIGN SPEC PROMPT 2 RESPONSE>, <SCREENS SPEC: DESIGN SPEC PROMPT 4 RESPONSE>

EXEMPLO DE PROMPT

. Gerar especificações de requisitos. Considere o aplicativo em Gestão documental. O contexto do aplicativo é documentos históricos. Abaixo estão descritos os requisitos de negócios do aplicativo - Os usuários devem cadastrar os documentos históricos, com informações de base como, nome, descrição, data de envio entre outras e deve anexar a imagem do documento, em JPG ou PNG. - O sistema deve receber as informações, salvar os dados no banco e a imagem no bucket Minio, ao mesmo tempo, é enviado o nome da imagem e agora, o id do documento, por meio de fila para o OCR; O OCR subscreve a fila, que, ao ver uma nova imagem, vai no bucket, pega a imagem, usa otesseract para transcrever o documento, faz uma limpeza, tokeniza e salva, os tokens, ligado ao id do documento, em um banco de dados não relacional. - O usuário, além de cadastrar documentos, pode buscar documentos pelo titulo, descrição ou ainda palavras chaves, estas, são palavras que foram estraídas do documento, por meio do OCR; - Como o OCR é lento, é necessário que o sistema suporte escalabilidade; - O usuário deve se autenticar no sistema para ter acesso; 2. Gere processos para os requisitos acima. Gere atividades para os processos juntamente com os parâmetros de entrada e saída. 3. Gere regras para os requisitos acima, abrangendo os seguintes tipos de regras: regras de controle de acesso, regras de lógica comercial, regras de cálculo, regras de conformidade, regras de validação de dados, regras de exibição, regras de notificação, regras de mudança de estado (transição) e regras de fluxo de trabalho. Por fim, monte um diagrama para representar a arquitetura cloud para OCI, por meio de código python, usando o diagrams para os requisitos acima.

RESULTADOS

- Código
- Requisitos
- Diagrama (gerado com o códito)



THANK YOU!

gomesrocha/
palestra_Developers_AI

0 Contributors | 0 Issues | 0 Stars | 0 Forks

gomesrocha/palestra_Developers_AI

Contribute to gomesrocha/palestra_Developers_AI development by creating an account on GitHub.