Desafio 1 - LLM sobre dados estruturados e não estruturados: extração de insights e predição

Descrição do problema de pesquisa

O desafio consiste em explorar e desenvolver modelos de linguagem natural (Large Language Models - LLMs) para a extração de insights e predição a partir de grandes volumes de dados estruturados (como bancos de dados e planilhas) e não estruturados (como textos, imagens e vídeos). A complexidade reside em integrar diferentes tipos de dados e extrair informações relevantes que possam auxiliar na tomada de decisão de usuários leigos que usam interfaces de chat simples para obter informações relevantes sobre seus dados.

Questões de pesquisa (lista não exaustiva)

- Como integrar eficientemente dados estruturados e não estruturados, de uma ou mais modalidade de tipo de dado, para inferência utilizando LLMs?
- Quais são as melhores práticas para a pré-processamento e limpeza de dados, multimodais ou não, para treinamento e refinamento de LLMs,?
- Como melhorar a precisão dos insights extraídos por LLMs com base na interpretabilidade das informações de várias fontes de dados?
- Quais técnicas podem ser aplicadas nos insights extraídos de dados heterogêneos produzidos por ML para incorporar informações semânticas trazidas de LLMs?
- Como automatizar a seleção de hiper-parâmetros de modelos preditivos, em conjunto com LLMs, para melhorar a generalização no aprendizado de dados estruturados e/ou não estruturados?
- Como melhorar dados espaciais enriquecido com informações semânticas para otimizar LLMs à compreensão de cenários tridimensionais?
- Como o treinamento de Large Language Models (LLMs) com dados multimodais não estruturados (texto e imagens) pode otimizar a geração de modelos 3D?

Desafio 2 - Cibersegurança baseada em IA Generativa

Descrição do problema de pesquisa

O desafio consiste em explorar e desenvolver soluções de cibersegurança utilizando IA generativa para identificar, prever e mitigar ameaças cibernéticas. A IA generativa pode ser utilizada para criar sistemas de defesa mais robustos e adaptáveis, capazes de responder a ameaças em tempo real e antecipar ataques antes que ocorram.

Questões de pesquisa (lista não exaustiva)

- Como a IA generativa pode ser utilizada para detectar e prevenir ataques cibernéticos em tempo real?
- Quais são as melhores práticas para a integração de IA generativa em sistemas de cibersegurança existentes?
- De que forma a IA generativa pode ser usada para identificar padrões de comportamento anômalos em redes de computadores?
- Como a automação de respostas a incidentes pode ser aprimorada utilizando modelos de IA generativa para reduzir o tempo de reação e mitigação?
- De que maneira a IA generativa pode contribuir para a criação de honeypots e outros sistemas de defesa que enganam e estudam os atacantes?
- Quais são as melhores práticas para a criação de modelos LLMs mais seguros utilizando como referência OWASP Top 10 for LLM?
- Como a IA generativa pode ser usada para prevenir e/ou mitigar Roubo de Identidade Digital?
- De que forma a IA generativa pode ser usada para identificar padrões de comportamento anômalos para prevenir e conter incidentes cibernéticos em ambientes de segurança de infraestruturas críticas?
- Como a IA Generativa pode ser usada na Cibersegurança Cibernética para estratégias e planos militares que respondem em tempo real a determinadas situações?
- De que modo a IA Generativa pode reforçar a segurança cibernética no sistema financeiro e detecção de fraudes no setor bancário?
- Como IA Generativa pode ser usada detectar crimes (bullying, racismo, pornografia, deep fakes, dentre outros) em ambientes virtuais?

Desafio 3 - Arcabouço para execução de inferência, refinamento e treinamento de modelos em dispositivos federados

Descrição do problema de pesquisa:

O desafio consiste em desenvolver um arcabouço para a execução de inferência, refinamento e treinamento de modelos de aprendizado de máquina em dispositivos federados. O objetivo é utilizar os recursos computacionais ociosos desses dispositivos (como smartphones, IoT, edge devices e servidores de nuvem) para a execução de cargas de trabalho de IA, permitindo que eles colaborem no treinamento e refinamento de modelos e realização de inferências. Isso deve ser feito preservando a privacidade dos dados e reduzindo a necessidade de transferência e processamento de grandes volumes de dados em servidores centrais.

Questões de pesquisa (lista não exaustiva)

- Como desenvolver um arcabouço que permita a execução eficiente de inferência de modelos em dispositivos federados com recursos limitados?
- Como otimizar a comunicação entre dispositivos federados para minimizar a latência e o consumo de largura de banda durante o processo de treinamento de modelos?
- Quais estratégias podem ser adotadas para a execução de cargas de trabalho de IA em dispositivos IoT de baixa capacidade, equilibrando eficiência energética e desempenho?
- Quais estratégias podem ser adotadas para balancear a carga de trabalho entre dispositivos federados, considerando as variações de capacidade de processamento e energia?
- Como maximizar a utilização de recursos computacionais ociosos em dispositivos federados para a execução de cargas de trabalho de IA sem impactar negativamente o desempenho do dispositivo para outras tarefas?
- Como otimizar o uso de recursos computacionais em dispositivos IoT para que a execução de tarefas de aprendizado de máquina não comprometa a funcionalidade principal do dispositivo, como sensores e atuadores?