**Grupo: Gabrieli, Guilherme, Neife e Raika**

**Computação Confidencial e Privacidade por Design**

A computação confidencial e a privacidade por design são abordagens que visam garantir a segurança dos dados durante o processamento e o armazenamento, minimizando riscos de vazamento e uso indevido. Essas técnicas são cada vez mais essenciais em um mundo onde dados pessoais e empresariais precisam ser protegidos contra acessos não autorizados.

Com o avanço da tecnologia, surgiram diversas abordagens e técnicas para aprimorar a proteção de dados, garantindo que a privacidade seja preservada desde a concepção dos sistemas até a sua utilização. Neste contexto, abordaremos alguns conceitos fundamentais que desempenham um papel importante na proteção da privacidade e na segurança dos dados:

* **Computação Homomórfica**: Permite realizar cálculos diretamente em dados criptografados, sem necessidade de descriptografá-los, garantindo maior segurança durante o processamento.
* **Federated Learning (Aprendizado Federado)**: Um método de aprendizado de máquina descentralizado que permite que modelos sejam treinados sem que os dados precisem sair dos dispositivos dos usuários.
* **Differential Privacy (Privacidade Diferencial)**: Uma abordagem estatística que adiciona ruído aos dados para dificultar a identificação de indivíduos em grandes conjuntos de informações.

A seguir, exploraremos cada um desses conceitos em detalhes.

**Computação Homomórfica**

A **computação homomórfica** é uma técnica criptográfica que permite a execução de operações em dados criptografados sem precisar descriptografá-los. Isso garante que informações sensíveis possam ser processadas com segurança, mesmo em ambientes não confiáveis.

Um dos principais avanços dessa tecnologia veio com o conceito de **criptografia homomórfica totalmente funcional (Fully Homomorphic Encryption - FHE)**, que permite qualquer tipo de operação matemática sobre dados criptografados. Um exemplo prático disso seria um serviço de saúde que armazena exames médicos criptografados e permite que algoritmos de IA façam análises sobre esses dados sem jamais acessá-los em sua forma original.

Empresas como **IBM e Microsoft** têm investido fortemente em computação homomórfica para criar soluções que possibilitam cálculos seguros em serviços de nuvem.

**Federated Learning (Aprendizado Federado)**

O **Aprendizado Federado (Federated Learning)** é uma abordagem de treinamento de modelos de inteligência artificial que permite que os dados permaneçam localizados nos dispositivos dos usuários, ao invés de serem centralizados em servidores. Isso melhora a privacidade e a segurança, pois os dados brutos nunca saem dos dispositivos.

Essa técnica foi popularizada pelo Google, que a utiliza em aplicativos como **Gboard**, onde o modelo de IA aprende padrões de digitação sem precisar acessar diretamente os textos digitados pelo usuário. Em vez disso, cada dispositivo treina um modelo localmente e apenas os parâmetros treinados são compartilhados com o servidor central, mantendo os dados privados.

Além de aumentar a privacidade, o aprendizado federado também reduz a necessidade de grandes volumes de transferência de dados, tornando-o mais eficiente para dispositivos móveis e IoT (Internet das Coisas).

**Privacidade por Design**

A privacidade diferencial é uma técnica que permite analisar dados coletados de um grupo de pessoas sem revelar informações sobre indivíduos específicos. Imagine que você tem um conjunto de dados com informações sobre a saúde de várias pessoas e deseja estudar a prevalência de uma determinada doença.

**Como funciona:**

1. **Adição de ruído:** A ideia principal é adicionar ruído aleatório aos resultados da análise. Esse ruído máscara as informações individuais, tornando difícil identificar se uma pessoa específica está presente no conjunto de dados ou qual é a sua informação.
2. **Controle do ruído:** A quantidade de ruído adicionada é cuidadosamente controlada para garantir que a análise ainda seja útil. Se o ruído for muito alto, os resultados serão imprecisos. Se for muito baixo, a privacidade será comprometida.
3. **Garantia de privacidade:** A privacidade diferencial fornece uma garantia matemática de que a presença ou ausência de uma pessoa no conjunto de dados não afetará significativamente os resultados da análise. Isso significa que é possível aprender sobre o grupo como um todo sem expor informações individuais.

**Exemplo:**

Imagine que você está analisando um conjunto de dados de saúde e deseja saber quantas pessoas têm diabetes. Em vez de fornecer o número exato, você pode adicionar um ruído aleatório. Por exemplo, se o número real for 100, você pode relatar um número entre 90 e 110.

**Benefícios:**

* **Proteção da privacidade:** A privacidade diferencial protege as informações individuais, mesmo que um invasor tenha acesso ao conjunto de dados e a outras informações sobre as pessoas.
* **Análise de dados útil:** Apesar da adição de ruído, a privacidade diferencial ainda permite obter resultados precisos e úteis para a análise de dados.
* **Aplicações:** A privacidade diferencial pode ser usada em diversas áreas, como saúde, pesquisa social e análise de dados governamentais.

Em resumo, a privacidade diferencial é uma ferramenta poderosa para proteger a privacidade individual ao mesmo tempo em que permite a análise de dados úteis.

Com o crescimento do uso de dados pessoais e sensíveis, as tecnologias de **computação confidencial**, **privacidade por design**, **computação homomórfica**, **aprendizado federado** e **privacidade diferencial** estão se tornando fundamentais para garantir a segurança e o sigilo das informações. Empresas e pesquisadores continuam desenvolvendo novas soluções para proteger os dados, equilibrando a necessidade de processamento e aprendizado com a proteção da privacidade dos usuários.