Privacy-Preserving Machine Learning with Federated Learning Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Federated Learning ile Gizlilik Odaklı Makine Öğrenmesi Eğitimi, hassas verilerin merkezi bir ortamda toplanmasının mümkün veya uygun olmadığı senaryolarda, **dağıtık makine öğrenmesi modellerinin** nasıl geliştirilebileceğini ele alan ileri düzey bir mühendislik ve araştırma programıdır.

Federated Learning (FL), farklı cihaz veya kuruluşlarda bulunan verileri merkezi bir sunucuya aktarmadan ortak bir **makine öğrenmesi modeli** eğitmeye olanak tanır. Bu yaklaşımda model, verinin bulunduğu ortamlarda eğitilir ve merkezi sisteme ham veri yerine **model güncellemeleri** iletilir.

Eğitim kapsamında, **FedAvg** algoritmasının çalışma döngüsünden başlayarak **Cross-Silo** ve **Cross-Device** mimarileri, merkezi ve merkeziyetsiz öğrenme yaklaşımları, **Non-IID Data (İstatistiksel Heterojenlik)** ve sistem kaynaklı farklılıklar incelenir.

Program ayrıca **FedProx** gibi heterojen veri dağılımlarına yönelik yöntemleri ve **Differential Privacy (DP)**, **Homomorphic Encryption (HE)** ve **Secure Multi-Party Computation (SMPC)** gibi **gizlilik artırıcı teknolojileri (Privacy-Enhancing Technologies – PETs)** ele alır.

Flower ve **TensorFlow Federated (TFF)** kütüphaneleriyle gerçekleştirilen uygulamalı çalışmalar sayesinde katılımcılar, veri gizliliğini gözeten dağıtık model eğitimi yaklaşımlarını deneyimleme fırsatı bulur.

Prerequisites

Bu eğitime katılım için herhangi bir **zorunlu ön koşul bulunmamaktadır**.

Who Should Attend

- **Veri Mahremiyeti Mühendisleri** ve **Güvenlik Mimarları**
- **Altyapı ve MLOps Mühendisleri**
- **Gömülü Sistemler** ve **Mobil Geliştirme Uzmanları**
- **Kıdemli Yapay Zekâ ve Makine Öğrenmesi Mühendisleri**
- **Makine Öğrenmesi Araştırmacıları**
- Sağlık, finans ve telekomünikasyon gibi hassas verilerle çalışan sektörlerdeki teknik uzmanlar
- **CTO'lar**, **Teknoloji Liderleri** ve **Ar-Ge Direktörleri**

Privacy-Preserving Machine Learning with Federated Learning Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Eğitimi tamamladığınızda:

- **Federated Learning** mimarisini ve merkezi makine öğrenmesinden farklarını açıklayabileceksiniz.
- Verilerin farklı sistemlerde kaldığı ortamlarda **ortak makine öğrenmesi modelleri** geliştirebileceksiniz.
- **FedAvg** algoritmasının çalışma döngüsünü ve **FedProx** yaklaşımının kullanım amacını anlayabileceksiniz.
- **Cross-Silo** ve **Cross-Device** Federated Learning mimarilerini karşılaştırabileceksiniz.
- **Non-IID veri dağılımları** ve **sistem heterojenliği** nedeniyle oluşan sorunları değerlendirebileceksiniz.
- **Differential Privacy, Homomorphic Encryption ve SMPC** gibi gizlilik artırıcı yöntemleri tanıyabileceksiniz.
- **GDPR, HIPAA ve KVKK** gibi düzenlemelerin veri gizliliğine yönelik gerekliliklerini mimari kararlarla ilişkilendirebileceksiniz.
- **Flower** ve **TensorFlow Federated** ile dağıtık model eğitimi çalışmalarını gerçekleştirebileceksiniz.
- Ham veriyi merkezi bir ortama taşımadan **model güncellemelerinin paylaşılmasına** dayalı sistemler tasarlayabileceksiniz.
- Hassas verilerin bulunduğu sektörlerde **gizlilik odaklı yapay zekâ çözümleri** geliştirmeye yönelik yaklaşımları değerlendirebileceksiniz.

Outline

1. Gizlilik Odaklı Yapay Zekânın Temelleri ve İhtiyaç Analizi

Geleneksel Merkezi Makine Öğrenmesinin Sınırlamaları

- **Merkezi makine öğrenmesi** yaklaşımının değerlendirilmesi
- **Veri mahremiyeti riskleri**
  - Veri sızıntıları
  - Verilerin ikincil amaçlarla kullanılması
  - Kimlik bilgilerinin açığa çıkması
- **GDPR, HIPAA ve KVKK** gibi düzenlemelerin veri merkezileştirme süreçleri üzerindeki etkileri
- **Veri siloları** nedeniyle ortaya çıkan iş birliği ve rekabet sorunları

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Gizlilik Artırıcı Teknolojiler (PETs)

- **Veri anonimleştirme** yöntemleri ve sınırlamaları
- **Yeniden kimliklendirme saldırıları (Re-identification Attacks)**
- **Differential Privacy (DP)**
- **Homomorphic Encryption (HE)**
- **Secure Multi-Party Computation (SMPC)**
- **Zero-Knowledge Proofs (ZKP)**
- **Federated Learning'in**, diğer gizlilik artırıcı teknolojilerle ilişkisi

2. Federated Learning Mimarisi ve Temel Algoritmalar

Federated Learning'in Çalışma Prensibi

- **Federated Learning** yaklaşımının temel bileşenleri
- Merkezi sunucu ile dağıtık **istemciler (Clients)** arasındaki işleyiş
- Modelin istemcilere dağıtılması
- Yerel veriler üzerinde model eğitimi
- **Model ağırlıklarının ve gradyan güncellemelerinin** paylaşılması
- Güncellemelerin birleştirilmesiyle **global modelin** geliştirilmesi

FedAvg Algoritması

- **Federated Averaging (FedAvg)** yaklaşımı
- Yerel eğitim ve merkezi model birleştirme döngüsü
- Ham veriyi paylaşmadan ortak model eğitimi

Federated Learning Mimarileri

- **Cross-Silo Federated Learning:** Kurumlar arasında ortak model eğitimi
- **Cross-Device Federated Learning:** Çok sayıda uç cihaz üzerinde model eğitimi
- **Merkezi Federated Learning**
- **Merkeziyetsiz (Peer-to-Peer / P2P) Federated Learning**
- **Hiyerarşik Federated Learning**

3. Federated Learning'in Temel Zorlukları: Heterojenlik

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- **Non-IID Data** kavramı
- İstemciler arasındaki **istatistiksel heterojenlik**
- Farklı veri dağılımlarının model eğitimine etkisi
- **Sistem heterojenliği**
  - İşlem gücü farklılıkları
  - Ağ bağlantısı farklılıkları
  - Cihaz ve altyapı kaynaklı sınırlamalar
- **İletişim darboğazları** ve ağ maliyetleri
- **FedProx** yaklaşımının heterojen veri koşullarındaki rolü

4. Güvenliğin Artırılması: Diferansiyel Gizlilik ve Kriptografik Yöntemler

Differential Privacy

- **Differential Privacy (DP)** kavramı
- Model güncellemelerine matematiksel gürültü eklenmesi
- Bireysel veri katkılarının açığa çıkma riskinin azaltılması

Kriptografik Gizlilik Yöntemleri

- **Homomorphic Encryption (HE)** ile şifreli veriler üzerinde işlem yapma yaklaşımı
- Model güncellemelerinin şifreli biçimde birleştirilmesi
- **Secure Multi-Party Computation (SMPC)** yaklaşımı
- **Federated Learning** ile gizlilik artırıcı teknolojilerin birlikte değerlendirilmesi

5. Uygulamalı Atölye: Flower ve TensorFlow Federated (TFF)

- **Flower** kütüphanesine giriş
- Python tabanlı ve farklı makine öğrenmesi framework'leriyle çalışabilen **Federated Learning** yaklaşımları
- **TensorFlow Federated (TFF)** kütüphanesinin incelenmesi
- Dağıtık model eğitiminin uygulamalı olarak değerlendirilmesi
- Yerel model eğitimi ve **global model güncellemeleri** üzerinde çalışmalar