

المفاهيم والمصطلحات الرئيسة

الذكاء الاصطناعي التوليدي وخصوصية البيانات

ستتعرف في هذا الدرس على المفاهيم والمصطلحات الرئيسة الآتية:

Data Privacy	خصوصية البيانات
Extraction Attacks	الهجمات الاستخراجية
Inference Attacks	التحليل الاستنتاجي
Federated Learning	التعلم الفيدرالي
Differential Privacy	الخصوصية التفاضلية
Encryption	التشفير
Homomorphic Encryption	التشفير المتجانس
Advanced Anonymization	إخفاء الهوية