المفاهيم والمصطلحات الرئيسة

الذكاء الاصطناعي التوليدي وخصوصية البيانات

ستتعرف في هذا الدرس على المفاهيم والمصطلحات الرئيسة الآتية:

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