الدورة التدريبية: التعلم الموحد - تعزيز خصوصية البيانات في الذكاء الاصطناعي (Federated Learning)



16 - 20 نوفمبر 2026
بوسطن
7500 € (للشخص الواحد)
Ref: #AI8066_322151

مقدمة الدورة التدريبية / لمحة عامة:

يقدم BIG BEN Training Center هذه الدورة التدريبية المتخصصة حول التعلم الموحد (Federated Learning): تعزيز خصوصية البيانات في الذكاء الاصطناعي، وهي مصممة لمهندسي الذكاء الاصطناعي، وعلماء البيانات، ومديري المنتجات، والمختصين في الأمن السيبراني والخصوصية، والباحثين الذين يسعون لتطوير نماذج ذكاء اصطناعي (AI) دون المساس بخصوصية البيانات. في عصر البيانات الضخمة، أصبحت الخصوصية والأمان من أكبر التحديات التي تواجه تطوير ونشر حلول الذكاء الاصطناعي، خاصة في القطاعات الحساسة مثل الرعاية الصحية والمالية. يوفر التعلم الموحد حلاً مبتكراً لهذه التحديات من خلال تمكين تدريب نماذج التعلم الآلي (Machine Learning) على مجموعات بيانات موزعة محلياً دون الحاجة إلى تجميع البيانات الخام في موقع مركزي. ستغطي الدورة مفاهيم التعلم الموحد الأساسية، وكيفية عمله، ومميزاته وتحدياته، وتطبيقاته العملية في سيناريوهات مختلفة، وتقنيات تعزيز الخصوصية المرتبطة به مثل الخصوصية التفاضلية (Differential Privacy) والتشفير المتماثل (Homomorphic Encryption). سيتعلم المشاركون كيفية تصميم وتنفيذ أنظمة التعلم الموحد، وتحسين أدائها، وضمان الامتثال لمتطلبات الخصوصية في مشاريعهم. تهدف الدورة إلى تمكين المختصين من فهم إمكانات التعلم الموحد، وبناء حلول ذكاء اصطناعي تحافظ على الخصوصية، والمساهمة في تطوير ممارسات الذكاء الاصطناعي الآمنة والمسؤولة. نستلهم في هذه الدورة من أعمال البروفيسور نيكولاس بابيرني (Nicolas Papernot)، Nicolas Papernot، أحد الرواد في مجال التعلم الموحد والخصوصية التفاضلية في الذكاء الاصطناعي، والذي يؤكد على أهمية خصوصية البيانات كعنصر أساسي في نشر الذكاء الاصطناعي على نطاق واسع. ستقدم الدورة أمثلة واقعية على كيفية تطبيق التعلم الموحد في الصناعات التي تتطلب أعلى مستويات الخصوصية، مما يعزز فهم المشاركين للجوانب العملية والتطبيقية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسي الذكاء الاصطناعي والتعلم الآلي.
- علماء البيانات.
- مهندسي البرمجيات.
- المختصين في أمن البيانات والخصوصية.
- مديري المنتجات في شركات التكنولوجيا.
- الباحثين في مجال الذكاء الاصطناعي.
- المدراء التقنيين.
- المختصين في الامتثال والتنظيم.
- مهندسي النظم الموزعة.
- المهتمين بالذكاء الاصطناعي المسؤول.

القطاعات والصناعات المستهدفة:

- الرعاية الصحية (حماية سجلات المرضى).
- الخدمات المالية (الأمن المصرفي، الكشف عن الاحتيال).
- الاتصالات (تحسين الخدمات دون تجميع البيانات).
- التكنولوجيا والمستهلك (لوحات المفاتيح الذكية، الأجهزة المحمولة).
- القطاع الحكومي (خصوصية المواطنين).
- السيارات (القيادة الذاتية الآمنة).
- التصنيع (الصيانة التنبؤية للآلات).
- البحث والتطوير.
- التجارة الإلكترونية (توصيات المنتجات).
- التأمين.

الأقسام المؤسسية المستهدفة:

- قسم الذكاء الاصطناعي والتعلم الآلي.
- قسم أمن المعلومات والخصوصية.
- قسم البحث والتطوير (R&D).
- قسم تطوير المنتجات.
- قسم الامتثال القانوني والتنظيمي.
- قسم علم البيانات.
- قسم هندسة البرمجيات.
- قسم إدارة البيانات.
- قسم الابتكار.
- قسم الاستراتيجية التقنية.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم المبادئ الأساسية للتعلم الموحد وكيفية عمله.
- التمييز بين التعلم الموحد وطرق التدريب الموزعة الأخرى.
- تحديد مميزات وتحديات تطبيق التعلم الموحد.
- استكشاف تطبيقات التعلم الموحد في مختلف الصناعات.
- فهم آليات الخصوصية التفاضلية ودورها في التعلم الموحد.
- التعرف على التشفير المتماثل وتطبيقاته في التعلم الموحد.
- تصميم معماريات التعلم الموحد لمشاريع واقعية.
- التعامل مع أدوات وأطر عمل التعلم الموحد (مثل TensorFlow Federated).
- تقييم المخاطر المتعلقة بالخصوصية والأمان في أنظمة التعلم الموحد.
- بناء نماذج ذكاء اصطناعي تحافظ على خصوصية البيانات بفعالية.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة على منهجية تدريبية متقدمة وتطبيقية، تهدف إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لبناء حلول ذكاء اصطناعي تحافظ على خصوصية البيانات باستخدام التعلم الموحد. تشمل المنهجية محاضرات نظرية معمقة حول المفاهيم الأساسية للتعلم الموحد والتقنيات المتقدمة لتعزيز الخصوصية، بالإضافة إلى ورش عمل عملية مكثفة. سيقوم المشاركون بتصميم وتنفيذ أنظمة تعلم موحد بسيطة، وفحص تحدياتها العملية، وتطبيق تقنيات مثل الخصوصية التفاضلية لحماية البيانات الحساسة. سيتم التركيز على دراسات حالة واقعية من الصناعات التي تتطلب خصوصية عالية، مما يعزز فهم المشاركين للجوانب العملية والتطبيقية للتعلم الموحد. تتضمن الدورة جلسات عمل جماعي لتطوير حلول مبتكرة لمشكلات خصوصية البيانات. يتلقى المشاركون تغذية راجعة مفصلة ومنتظمة من المدربين الخبراء لضمان تطوير مهاراتهم في هذا المجال الحيوي والمتطور.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: مقدمة إلى التعلم الموحد ومبادئه.

- مفهوم التعلم الموحد (Federated Learning) ونشأته.
- الحاجة إلى التعلم الموحد: تحديات الخصوصية وأمن البيانات.
- الفرق بين التعلم الموحد والتعلم الموزع التقليدي.
- كيف يعمل التعلم الموحد: نظرة عامة على سير العمل.
- أنواع معماريات التعلم الموحد (Cross-device, Cross-silo).
- مميزات التعلم الموحد (الخصوصية، الكفاءة، اللامركزية).
- تحديات التعلم الموحد (عدم تجانس البيانات، التواصل، الأمان).

الوحدة الثانية: تقنيات تعزيز الخصوصية في التعلم الموحد.

- الخصوصية التفاضلية (Differential Privacy): المبادئ والتطبيقات.
- إضافة الضوضاء (Noise Injection) لحماية خصوصية البيانات.
- التشفير المتماثل (Homomorphic Encryption) ودوره في التعلم الموحد.
- الحساب الآمن متعدد الأطراف (Secure Multi-Party Computation - SMPC).
- الهندسة المعمارية لحماية الخصوصية في التعلم الموحد.
- مقارنة بين تقنيات تعزيز الخصوصية.
- تنفيذ الخصوصية التفاضلية في نماذج التعلم الموحد.

الوحدة الثالثة: تصميم وتطبيق أنظمة التعلم الموحد.

- اختيار النموذج والخوارزمية المناسبة للتعلم الموحد.
- إدارة البيانات غير المتجانسة في بيئات التعلم الموحد.
- استراتيجيات تجميع النماذج (Aggregation Strategies).
- تحسين التواصل والكفاءة في التعلم الموحد.
- أطر عمل التعلم الموحد (TensorFlow Federated, PySyft).
- بناء أول نظام تعلم موحد بسيط.
- استكشاف حالات الاستخدام العملية للتعلم الموحد.

الوحدة الرابعة: تطبيقات عملية للتعلم الموحد في الصناعات.

- التعلم الموحد في الرعاية الصحية والتشخيص الطبي.
- التعلم الموحد في الخدمات المالية والكشف عن الاحتيال.
- التعلم الموحد في الأجهزة المحمولة ولوحات المفاتيح الذكية.
- التعلم الموحد في أنظمة القيادة الذاتية.
- التعلم الموحد في تطبيقات المدن الذكية.
- التعلم الموحد في قطاع الاتصالات.
- تحديات خاصة بكل قطاع وكيفية معالجتها بالتعلم الموحد.

الوحدة الخامسة: مستقبل التعلم الموحد، التحديات، والاعتبارات الأخلاقية.

- التطورات الحديثة والاتجاهات المستقبلية في التعلم الموحد.
- التحديات البحثية المفتوحة في التعلم الموحد.
- الامتثال التنظيمي والخصوصية (GDPR, HIPAA).
- الاعتبارات الأخلاقية للتعلم الموحد (التحيز، العدالة).
- الذكاء الاصطناعي المسؤول (Responsible AI) ودور التعلم الموحد.
- تأثير التعلم الموحد على الابتكار في الذكاء الاصطناعي.
- الخطوات التالية للمهنيين في مجال التعلم الموحد.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

مع تزايد الاعتماد على التعلم الموحد كحل لخصوصية البيانات في تطوير نماذج الذكاء الاصطناعي، كيف يمكن للمطورين والمنظمين ضمان تحقيق التوازن الأمثل بين الحفاظ على سرية المعلومات الفردية وتحقيق أقصى استفادة من البيانات الموزعة لتحسين أداء النماذج، مع الأخذ في الاعتبار التعقيدات التقنية والتحديات الأخلاقية؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتقديمها تخصصاً عميقاً في التعلم الموحد، وهو مجال حيوي ومتزايد الأهمية في سياق خصوصية البيانات وأمن الذكاء الاصطناعي. ما يميزنا هو التركيز على الجانب العملي والتطبيقي لبناء أنظمة ذكاء اصطناعي تحافظ على الخصوصية، مع دمج أحدث التقنيات لتعزيز الأمان مثل الخصوصية التفاضلية والتشفير المتماثل. نغطي جميع الجوانب الأساسية والمتقدمة للتعلم الموحد، من مبادئه الأساسية إلى تصميمه وتطبيقاته في مختلف الصناعات الحساسة. الدورة تركز على تزويد المشاركين بالمهارات اللازمة للمساهمة بفاعلية في مشاريع الذكاء الاصطناعي التي تتطلب معالجة آمنة للبيانات، وقيادة مبادرات الابتكار مع الالتزام بالخصوصية، مما يجعلها ضرورية لأي محترف يسعى ليكون رائداً في هذا المجال المعقد والمطلوب.