



أكاديمية جوعان بن جاسم للدراسات الدفاعية
Joan Bin Jassim Academy for Defence Studies

الذكاء الاصطناعي والأمن السيبراني

MSCS 640 - خريف 2026

المقرر الدراسي

الذكاء الاصطناعي والأمن السيبراني	المقرر:
MSCS 640	الرمز:
ماجستير العلوم في الدفاع السيبراني	البرنامج:
إلزامي	النوع:
غرفة المختبر	القسم:
الاثنين 17:00-20:00	التوقيت:
3	الساعات المعتمدة:
https://courses.karbab.net/mscs640/	الصفحة:
د. المعتز بالله قرياب	المحاضر:
mouatez@karbab.net	البريد الإلكتروني:

الوصف

يقدم هذا المقرر دراسة دقيقة وعملية لتصميم وتطوير ونشر حلول الذكاء الاصطناعي (AI) الذكية المصممة لمواجهة التحديات الملحة في الأمن السيبراني الحديث. تم تصميم هذا المقرر لتزويد الطلاب بالأسس النظرية والمهارات التقنية التطبيقية اللازمة لوضع تصور وتنفيذ وتشغيل أنظمة دفاعية مدفوعة بالذكاء الاصطناعي ضمن بيئات أمنية معقدة وديناميكية. يبدأ المنهج بمقدمة منهجية للبادئ التأسيسية، مما يضمن اكتساب الطلاب فهماً واضحاً ومنظماً للمفاهيم الأساسية في الذكاء الاصطناعي والأمن السيبراني. يعمل المقرر على بناء التعلم تدريجياً من التعريفات الأساسية إلى المنهجيات المتقدمة. خلال المقرر، تعمل لغة بايثون كلغة برمجة أساسية، تكملها مكتبات تعلم الآلة والتعلم العميق المستخدمة على نطاق واسع. يتيح هذا النهج للطلاب اكتساب خبرة عملية في تنفيذ أحدث الخوارزميات والتقنيات لمجموعة متنوعة من التطبيقات الأمنية، بما في ذلك اكتشاف التصيد الاحتيالي، وتحليل اقتحام الشبكات، واكتشاف الحالات الشاذة، وتصنيف البرامج الضارة. بالإضافة

إلى التنفيذ الفني، يؤكد المقرر على الأبعاد التشغيلية والتنظيمية الأوسع لنشر الذكاء الاصطناعي في سياقات الأمن السيبراني. سيتناول الطلاب موضوعات مثل عمليات تعلم الآلة (MLOps) وإدارة دورة حياة نماذج الذكاء الاصطناعي، وضرورة التحقق المستمر في بيئات التهديدات العدائية والمتطورة بسرعة. علاوة على ذلك، يتناول المقرر الاعتبارات الأخلاقية والقانونية والحوكمة، مما يشجع الطلاب على التفكير النقدي في قضايا مثل العدالة الخوارزمية، والشفافية، والمساءلة، والتأثير المجتمعي للأنظمة الأمنية التي تدعم الذكاء الاصطناعي. من خلال دمج الرؤى النظرية، وتنمية المهارات التقنية، والتفكير النقدي، يهدف هذا المقرر إلى إعداد الطلاب للمساهمة بشكل هادف في المجال الناشئ للأمن السيبراني المدفوع بالذكاء الاصطناعي، سواء في البحث أو الصناعة أو سياقات صنع السياسات.

الأهداف

عند الانتهاء بنجاح من هذا المقرر، سيتمكن الطلاب من:

1. إظهار فهم أساسي للمفاهيم الأساسية في الذكاء الاصطناعي (AI) والأمن السيبراني، وشرح العلاقات المتبادلة بينهما.
2. تصميم وتدريب وتقييم نماذج الذكاء الاصطناعي لمهام مثل اكتشاف التصيد الاحتيالي، وتحليل اختراق الشبكات، واكتشاف الحالات الشاذة، وتصنيف البرامج الضارة.
3. تطبيق برجة بايثون ومكتبات تعلم الآلة/التعلم العميق المستخدمة على نطاق واسع لتنفيذ حلول قائمة على الذكاء الاصطناعي لتحديات الأمن السيبراني.
4. تقييم نقدي للمتطلبات التشغيلية لنشر الذكاء الاصطناعي في أنظمة الأمان في العالم الحقيقي، بما في ذلك إدارة دورة حياة النموذج، والتحقق المستمر، والقدرة على التكيف مع التهديدات المتطورة.
5. دمج المعرفة النظرية والمهارات التقنية والوعي الأخلاقي لاقتراح وتنفيذ استراتيجيات تدعم الذكاء الاصطناعي للدفاع ضد التهديدات السيبرانية.

مخرجات التعلم

عند إتمام هذا المقرر، سيتمكن الطلاب من:

1. بناء أنظمة كشف قائمة على الذكاء الاصطناعي: تطوير وتحسين نماذج عملية لتعلم الآلة باستخدام Python والمكتبات القياسية (مثل Scikit-learn و TensorFlow و PyTorch) للكشف عن

تهديدات سيبرانية محددة، تشمل محاولات التصيد الاحتيالي، وبصمات البرامج الضارة، والحالات الشاذة في الشبكات.

2. هندسة مسارات متكاملة لتعلم الآلة: تنفيذ مسارات بيانات كاملة ملائمة للسياقات الأمنية، مع إظهار الكفاءة في المعالجة المسبقة للبيانات، وهندسة السمات، وتدريب النماذج داخل إطار عملي للأمن السيبراني.

3. تشغيل نماذج الدفاع (MLOps): تصميم استراتيجيات للنشر تتضمن أفضل ممارسات MLOps، مع التركيز على إدارة دورة حياة النموذج، والمراقبة المستمرة للأداء، وإعادة تدريب النماذج استجابة لانحراف بيانات التهديدات.

4. تقييم متانة النماذج وفعاليتها: التقييم النقدي لأداء الحلول الدفاعية القائمة على الذكاء الاصطناعي في ضوء مقاييس واقعية وظروف عدائية، لتحديد جدواها التشغيلية وحدودها في بيئة أمنية حقيقية.

5. صياغة استراتيجيات الحوكمة الأخلاقية: تحليل الآثار الأخلاقية والقانونية والمجتمعية لنشر الذكاء الاصطناعي في الأمن السيبراني، بما يتيح وضع أطر للحوكمة تضمن العدالة الخوارزمية والمساءلة والشفافية.

المواد التعليمية

• إلزامي : الأمن السيبراني المدعوم بالذكاء الاصطناعي: بناء أنظمة دفاع ذكية، التقنيات والتطبيقات المعترز بالله قرباب (2026) (<https://books.karbab.net/ai-cybersec/>)

• اختياري: Cybersecurity for Intelligence Artificial Hands-On A. Parisi, (2019).

• اختياري: Cybersecurity for Learning Machine Hands-On S. Ozdemir, & S., Halder, (2018).

• اختياري: TensorFlow and Keras, Scikit-Learn, with Learning Machine Hands-On A. Géron,

المنهجية

يتضمن هذا المقرر محاضرات ومناقشات وتطبيقات عملية وأنشطة جماعية وأبحاث وتقارير أكاديمية. يساهم المتعلمون في العملية التعليمية من خلال المشاركة في قراءة وتحليل الأبحاث المتعلقة بموضوعات المحاضرات وإثراء النقاش من خلال التقييم النقدي للأبحاث والمواد العلمية المقترحة. سيتم توفير المادة العلمية للمقرر، بالإضافة

إلى المراجع والأبحاث المختلفة، للمتعلمين على المنصة الإلكترونية حتى يتمكنوا من الاطلاع عليها وإتاحة الفرصة لهم من خلال المحاضرات الأسبوعية لاستيعاب المفاهيم المختلفة ومناقشة القراءات. من المتوقع أن يساهم المتعلم بنشاط في العملية التعليمية وسيتم تقييم الأنشطة المختلفة المتعلقة بالمقرر مثل المشاركة أثناء المحاضرات، والمناقشة النقدية للبحوث، والواجبات النظرية والعملية.

الأنشطة

- ضرورة المشاركة الفعالة في الفصل وفي فرق العمل المختلفة، والانتظام في حضور المحاضرات واحترام مواعيدها بداية ونهاية، وكذلك عدم استخدام الهواتف المحمولة والهواتف وعدم تبادل الأحاديث الجانبية.
- يجب على جميع المتعلمين الاهتمام الشديد بإكمال وتقديم المتطلبات في الوقت المحدد.
- يجب على جميع المتعلمين التعامل مع القراءات الأسبوعية الإضافية بعناية فائقة لفهم وتحليل وتطوير معارفهم من خلال البحث عن مصادر أخرى.
- يجب على جميع المتعلمين تكوين ملف للمادة.
- من المتوقع أن يقوم المتعلمون بتدوين المعرفة اللازمة أثناء المحاضرة.

العملية التعليمية

1. مشاركة المتعلم تعتبر المشاركة في الفصل وحضور المحاضرات عنصراً نشطاً لكل طالب في أكاديمية جوعان بن جاسم للدراسات الدفاعية، ومن المتوقع أن يحضر الطالب جميع المحاضرات. إذا تجاوز الطالب النسبة المئوية المسموح بها للغياب وهي 25٪، فسيحصل على درجة رسوب بغض النظر عن أدائه. تقع على عاتق الطالب مسؤولية مراقبة حضوره. سيتم تسجيل الحضور اعتباراً من اليوم الأول للدراسة، بغض النظر عن الفترة المخصصة للحذف والإضافة.

2. انتهاك الحقوق الفكرية والمعنوية

يعتبر انتهاك الحقوق الفكرية والمعنوية إساءة أكاديمية وقد يؤدي إلى فقدان الدرجات أو الرسوب. تشمل هذه الانتهاكات القضايا التالية وتنطبق على جميع أعمال المتعلمين:

- استخدام أعمال أو أفكار أو صور أو كلمات أي شخص آخر دون إذنه أو دون الإشارة إلى المصدر.
- استخدام اسم شخص آخر أو جملة أو فقرة أو مقال دون استخدام علامات الاقتباس.

• سوء استخدام المصادر المستخدمة.

3. حالات التأخر في التسليم أو عدم تسليم الواجبات

- الطالب الذي لم يتمكن من حضور الامتحان أو تقديم المشروع أو تقديم العروض التقديمية في الوقت المحدد دون إذن أو عذر طبي، ستكون درجة التقييم في ذلك الجزء وفقاً لللائحة إجراءات أكاديمية جوعان بن جاسم للدراسات الدفاعية.
- إذا لم يتمكن المتعلم من القيام بواجب ما بسبب عذر مقبول، فسيحصل على درجة "غير مكتمل" في ذلك التقييم وسيتم منحه تقييماً آخر أو فترة تمديد.

4. السلوك

تتوقع الأكاديمية من المتعلمين الالتزام بمعايير عالية من قواعد السلوك في تفاعلهم مع أساتذة المقرر وزملائهم ومجتمع الأكاديمية، وفقاً لللائحة إجراءات أكاديمية جوعان بن جاسم للدراسات الدفاعية.

التقييم والدرجات

سيتم استخدام عدد من أدوات التقييم المختلفة لقياس مدى تحقيق مخرجات التعلم المذكورة أعلاه، بما في ذلك الاختبارات والمشاركة في الفصل والمختبرات.

أداة التقييم	التوقيت	الدرجة
المشاركة	خلال الفصل الدراسي	15
المختبرات	خلال الفصل الدراسي	15
المشروع	التسليم في الأسبوع 12	30
الاختبار النهائي	الأسبوع 15	40
المجموع		100

مقياس الدرجات:

النقاط المكتسبة	النسبة المئوية	الوصف	التقدير
4,00	100-90	ممتاز	A
3,50	85 إلى >90	جيد جداً (مرتفع)	B+
3,00	80 إلى >85	جيد جداً	B
2,50	75 إلى >80	جيد (مرتفع)	C+
2,00	70 إلى >75	جيد	C
0,00	أقل من 70	راسب	F
		ناجح	P+
		ناجح	P
		غير مكتمل	I
		مقرر مستمر	IP
		تحويل ساعات معتمدة	TC
		منسحب	W
		منسحب إجباري	WF
		مستمع	AU

مصادر التعلم والبحث

يجب على جميع الطلاب التسجيل في مكتبة قطر الوطنية (<https://www.qnl.qa/en>)، والتي توفر الوصول إلى معظم قواعد البيانات الإلكترونية الدولية في جميع التخصصات العلمية واللغات. يمكن العثور على قواعد البيانات ذات الصلة على <https://qnl.libguides.com/az.php>، بما في ذلك "دار المنظومة" و "المنهل" وقواعد بيانات الأطروحات والرسائل باللغة العربية. توفر المكتبة أيضاً الوصول إلى قواعد بيانات مشهورة مثل Taylor & Francis و ProQuest و Database Military و JSTOR و Sage Journals.

جدول المقرر

هذا الجدول مبدئي وقابل للتغيير حسب تقدير المحاضر.

الأسبوع	الموضوع	القراءات
الأسبوع 1	أسس الأمن السيبراني المدفوع بالذكاء الاصطناعي مختبر: بايثون لتعلم الآلة وتحليلات البيانات	الفصل 1
الأسبوع 2	أساسيات تعلم الآلة للأمن السيبراني، كاشف رسائل التصيد الاحتيالي مختبر: كاشف رسائل التصيد الاحتيالي من البداية إلى النهاية	الفصل 3 الفصل 4
الأسبوع 3	كشف التسلل إلى الشبكة القائم على تعلم الآلة مختبر: كشف التسلل إلى الشبكة من البداية إلى النهاية	الفصل 5 الفصل 6
الأسبوع 4	التعلم العميق لتحليل البرامج الضارة مختبر: كشف البرامج الضارة من البداية إلى النهاية موعد تسليم مقترح المشروع النهائي	الفصل 7
الأسبوع 5	الذكاء الاصطناعي لأمن الشبكات داخل المركبات مختبر: كشف التسلل إلى ناقل CAN	الفصل 8
الأسبوع 6	الذكاء الاصطناعي لأمن أجهزة الاستشعار في أنظمة CPS مختبر: سلامة أجهزة الاستشعار في أنظمة CPS	الفصل 9
الأسبوع 7	المحاولات من أجل معالجة اللغة الطبيعية الأمنية المتقدمة مختبر: كشف رسائل البريد الإلكتروني الضارة باستخدام المحولات	الفصل 10
الأسبوع 8	نماذج التسلسل للكشف عن الحالات الشاذة الزمنية مختبر: كشف السفر المستحيل	الفصل 11
الأسبوع 9	الطرق غير الموجهة للكشف عن هجمات اليوم صفر مختبر: كشف هجمات اليوم صفر والهجمات الجديدة	الفصل 12
الأسبوع 10	الشبكات العصبية للرسوم البيانية لتحليل العلاقات مختبر: شبكات GNN لكشف تهديدات الأمن السيبراني	الفصل 13
الأسبوع 11	عمليات تعلم الآلة في الأمن السيبراني مختبر: عمليات تعلم الآلة، كشف التسلل	الفصل 15
الأسبوع 12	تقييم النموذج والتحقق المستمر مختبر: تقييم النموذج وكشف الانحراف في مركز العمليات الأمنية	الفصل 16
الأسبوع 13	الخصوصية والأخلاق والحكمة في الذكاء الاصطناعي مختبر: بناء نظام كشف التسلل للشبكة (NIDS) عادل ومراعٍ للخصوصية موعد تسليم المشروع النهائي	الفصل 17
الأسبوع 14	التوجهات المستقبلية والمواضيع المتقدمة مختبر: تعلم الآلة العدائي في الأمن السيبراني	الفصل 18
الأسبوع 15	الاختبار النهائي	