Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB6063 Gr. 01
Titre : Méthodes avancées en cybersécurité basée sur l'intelligence artificielle
Session : Automne 2025 Horaire et local mercredi de 8h30 à 11h30
Professeure : Moudoud, Hajar

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e sera en mesure d'appliquer des techniques d'intelligence artificielle pour la cybersécurité ainsi que la sécurisation des systèmes basés sur l'intelligence artificielle.

Contenu

Éléments de base de l'intelligence artificielle (IA). Application des techniques d'apprentissage automatique et de raisonnement pour la sécurité des systèmes informatisés : détection de vulnérabilités, détection d'intrusions, classification de malwares, identification et analyse de risques. Systèmes d'attaques et de défenses autonomes basés sur l'IA. Étude des vulnérabilités des algorithmes de l'IA : empoisonnement des données, inférence des données d'apprentissage, inférence des paramètres de modèles, etc. Protection des technologies basées sur l'IA : confidentialité différentielle, génération d'exemples antagonistes, etc.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

Objectifs spécifiques du cours

À l'issue de ce cours, l'étudiant.e sera en mesure de :

- **Maîtriser les fondements de l'intelligence artificielle appliqués à la cybersécurité**, notamment les concepts clés en apprentissage automatique, en raisonnement automatisé et en traitement de données.
- **Mettre en œuvre des techniques d'IA pour la détection et la prévention d'attaques** telles que :
  - la détection d'intrusions,
  - l'identification de vulnérabilités logicielles,
  - la classification de malwares,
  - l'analyse automatisée des risques.
- **Analyser et concevoir des systèmes de défense autonomes** capables de s'adapter et de réagir en temps réel à des menaces évolutives grâce à l'IA.
- **Comprendre et évaluer les vulnérabilités spécifiques des algorithmes d'IA**, telles que :
  - l'empoisonnement de données (data poisoning),
  - l'inférence des données d'apprentissage,
  - l'extraction de modèles (model inversion, model stealing).
- **Développer des stratégies de protection des systèmes basés sur l'IA**, incluant :
  - l'application de la confidentialité différentielle,
  - la détection et la génération d'exemples antagonistes (adversarial examples),
  - la robustesse des modèles face aux attaques ciblées.

3. Stratégies pédagogiques :

- Cours en supervision, accompagnés de travaux pratiques.
- Examen de mi-session (en présentiel).
- Examen final (en présentiel).

Les étudiant(e)s qui s'inscrivent à ce cours doivent s'assurer qu'ils ont accès à : un ordinateur.
Le matériel pédagogique est accessible à partir de la plateforme Moodle dédiée au cours. Un forum de discussion sera aussi disponible pour poser des questions liées à la matière enseignée.

4. Heures de disponibilité ou modalités pour rendez-vous :

Communication par courriel (hajar.moudoud@uqo.ca) et via le forum de discussion. Période de consultation flexible (lundi au vendredi) sur rendez-vous seulement (prévoir 48 heures d'avance pour la prise de rendez-vous).

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Présentation du plan de cours, des activités évaluées, introduction et mise en contexte	03 sep. 2025
2	Concepts de base et fondamentaux de l'IA pour la cybersécurité	10 sep. 2025
3	Pré-traitement des données et régression	17 sep. 2025
4	Fondamentaux de l'IA pour la cybersécurité	24 sep. 2025
5	Classification des attaques et étude de cas (KNN-SVM-NB)	01 oct. 2025
6	Détection d'intrusions par apprentissage automatique **Révisions pour l'examen de mi-session**	08 oct. 2025
7	**Semaine d'études**	14 au 17 oct. 2025
8	**Examen de mi-session**	**22 oct. 2025**
9	Intelligence artificielle adversaire et robustesse	29 oct. 2025
10	Analyse de risques et systèmes de défense autonomes	05 nov. 2025
11	Vulnérabilités des algorithmes d'IA	12 nov. 2025
12	Confidentialité, éthique et IA explicable	19 nov. 2025
13	Sécurisation des systèmes basés sur l'IA **Révisions pour l'examen final**	26 nov. 2025
14	Présentation orale des projets de session	03 déc. 2025
15	**Examen final**	**10 déc. 2025**

6. Évaluation du cours :

Cette section renseigne l'étudiante et l'étudiant quant aux différentes évaluations (ex. : travaux et examens) qui auront lieu au cours du trimestre. Voir le tableau des évaluations ci-dessous.

DATE LIMITE d'abandon de cours sans mention d'échec : 28 octobre 2025.

Veuillez noter : Pour chaque activité évaluée, un énoncé sera remis quelques jours avant le début de la période consacrée à celui-ci. En plus de l'énoncé, vous recevrez les fichiers avec lesquels vous devrez travailler et un briefing vous sera donné à ce sujet. Pour les examens, l'énoncé est intégré à la question. Avant chaque examen, il y aura une séance où l'enseignant résoudra des problèmes similaires à ceux que vous aurez à l'examen.

ChatGPT et autres outils génératifs : Les solutions requises pour les TP et dans les examens se prêtent mal à l'utilisation des outils génératifs. Vous devez traiter les résultats de cette utilisation comme une citation dans le texte et dans la médiagraphie.

Activité évaluée	Mode et date-heure buttoir	%age de la note finale
Projet 1	Remise avant le 24 sep à 23h00, Moodle	10%
Projet 2	Remise avant le 08 oct. à 23h00, Moodle	10%
Projet 3	Remise avant le 12 nov. à 23h00, Moodle	10%
Examen intra	Individuel, le 22 oct.	20%
Travail de session	Remise avant le 03 déc. à 23h00, Moodle	20%
Examen final	Individuel, le 10 déc.	30%

La qualité de la langue

Travaux pratiques : Les rapports relatifs aux travaux pratiques doivent être rédigés dans un français intelligible et exempt d'anglicismes. Pour vous aider au niveau des anglicismes, veuillez consulter le site de l'Office de la langue française du Québec au https://www.oqlf.gouv.qc.ca/accueil.aspx. Tout terme accepté comme étant du bon français par cet organisme sera considéré comme correct au niveau de la correction. Les trois ouvrages de de Villers cité dans la bibliographie (section 16 ci-dessous) viennent compléter le site de l'OQLF pour les corrections.
Examens : La rédaction d'examen se faisant avec une contrainte de temps, on ne peut exiger des étudiant(e)s le même niveau de français que pour les travaux pratiques. En revanche, une réponse incohérente ou inintelligible ne peut déboucher sur la certitude que la matière a été bien comprise. La qualité du français utilisé par l'élève lors de l'examen doit donc être tel que le correcteur puisse évaluer efficacement cette compréhension de la matière.

Règles de présentation des travaux

Le numéro de l'équipe et les noms des équipiers doivent apparaître en page 1 de tout rapport remis. Les rapports relatifs aux travaux pratiques doivent utiliser le formulaire mis à la disposition des équipes. Les réponses demandées peuvent varier en longueur, allant d'un seul mot à plusieurs lignes. Chaque question doit être répondue indépendamment des autres questions. Les réponses doivent être aussi concises mais aussi précises que possible. Les réponses inutilement longues ne seront pas corrigées car il n'appartient pas au correcteur de choisir les éléments utiles de la réponse parmi les éléments inutiles.

Règles concernant les retards dans la remise des travaux

Les dates des remises des rapports des travaux pratiques sont connues dès le début de la session. Il appartient donc à l'étudiant(e) de planifier correctement la quantité de travail à mettre sur le travail pratique ainsi que le moment où appliquer cet effort. Lorsqu'un travail est remis après la date d'échéance, l'équipe perd 5% pour chaque heure de retard. La remise est considérée en retard lorsque l'heure est commencée (donc : un retard d'une minute est considéré comme une heure de retard). Si l'équipe sait que la remise ne fera pas en temps, elle peut prendre entente avec l'enseignant et convenir d'un nouveau moment pour la remise et de la pénalité qui résultera du retard. Le délai convenu et la pénalité doivent être raisonnables compte tenu des circonstances.

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude. L'utilisation d'un logiciel de médiagraphie comme Zotéro est fortement suggérée.

- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)
- Politique sur la liberté académique

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.
Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.
Ensemble, participons à une culture de respect.
Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

Les références seront fournies pendant le cours.

9. Page Web du cours :

https://moodle.uqo.ca