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 2024 Horaire et local
Professeur.e : Bouhaddi, Myria

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 :

3. Stratégies pédagogiques :

La structure pédagogique de ce cours intègre les éléments suivants :

1. **Cours magistraux** : une séance hebdomadaire de 3 heures.
2. **Devoirs** : répartis tout au long du semestre pour renforcer les concepts abordés.
3. **Projet avec présentation orale** : permettant aux étudiants de démontrer leur compréhension et d'appliquer les connaissances acquises.
4. **Deux examens** : Évaluant la maîtrise des compétences et des connaissances couvertes en cours.

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

Communication par courriel (myria.bouhaddi@uqo.ca) et via le forum de discussion.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Introduction à la cybersécurité et à l'intelligence artificielle** • Introduction au cours et présentation des concepts de base de la cybersécurité et de l'IA. • Aperçu des défis de la cybersécurité et du rôle de l'IA dans ce domaine.	06 sep. 2024
2	**Fondements de l'apprentissage automatique pour la cybersécurité** • Principes de l'apprentissage automatique : supervision, non-supervision, par renforcement. • Introduction aux algorithmes courants : régression logistique, SVM, arbres de décision. • Étude de cas : détection d'anomalies dans les systèmes informatisés.	13 sep. 2024

3	**Techniques avancées en apprentissage profond** • Réseaux neuronaux profonds, CNN, RNN, GANs. • Applications de l'apprentissage profond dans la détection de malwares et d'intrusions. • Étude de cas : Utilisation des CNN pour la classification des malwares. **Devoir 1**	20 sep. 2024
4	**Jour férié**	27 sep. 2024
5	**Détection d'anomalies et de vulnérabilités** • Techniques d'apprentissage non supervisé : clustering, détection d'anomalies. • Application à la détection d'intrusions réseau et d'anomalies de systèmes. • Étude de cas : Détection d'anomalies réseau avec K-means.	04 oct. 2024
6	**Classification des malwares et analyse de risques** • Techniques de classification supervisée et non supervisée pour la détection de malwares. • Méthodologies d'analyse de risques basées sur l'IA. • Étude de cas : Développement d'un modèle de classification de malwares.	11 oct. 2024
7	**Semaine d'études**	18 oct. 2024
8	**Examen de mi-session**	25 oct. 2024
9	**Systèmes d'attaques automatisés basés sur l'IA** • Modèles et stratégies d'attaques automatisées utilisant l'IA. • Analyse des exemples adversaires et des attaques par empoisonnement. • Étude de cas : simulation d'une attaque par génération d'exemples adversaires.	01 nov. 2024
10	**Systèmes de défense automatisés basés sur l'IA** • Techniques de défense autonomes et réactives basées sur l'IA. • Détection et réponse automatique aux menaces. • Étude de cas : Développement d'un système de défense basé sur l'apprentissage automatique.	08 nov. 2024
11	**Vulnérabilités des modèles d'IA - Partie 1** • Empoisonnement des données : introduction et contre-mesures. • Analyse des risques liés à l'inférence des données d'apprentissage. • Étude de cas : Analyse d'une attaque par empoisonnement des données. **Devoir 2**	15 nov. 2024

12	**Vulnérabilités des modèles d'IA - Partie 2** • Inférence des paramètres de modèles : vulnérabilités et techniques de défense. • Protection contre les attaques adversariales. • Étude de cas : Développement de défenses contre les attaques d'inférence.	22 nov. 2024
13	**Protection des technologies basées sur l'IA - Partie 1** • Introduction à la confidentialité différentielle et à son application dans l'IA. • Techniques pour garantir la sécurité des modèles d'apprentissage automatique. • Génération d'exemples antagonistes pour la protection des modèles.	29 nov. 2024
14	**Présentation orale des projets**	06 déc. 2024
15	**Examen final**	13 déc. 2024

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs des cours et des programmes.

Dans le cas spécifique du cours **Méthodes avancées en cybersécurité basée sur l'intelligence artificielle,** l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session : 30 %**
- **Examen final : 30 %**
- **Travail de session : 25 %**
- **Devoir 1 et 2 : 15 %**

Une moyenne inférieure à 50 % aux examens est éliminatoire et conduit automatiquement à un échec.

7. Politiques départementales et institutionnelles :

- Politiques relatives à la tenue des examens
- Note sur le plagiat et les fraudes
- 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)

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 :

1. Diogenes, Yuri, and Erdal Ozkaya. *Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics*. Packt Publishing Ltd, 2018.
2. Chio, Clarence, and David Freeman. Machine learning and security: Protecting systems with data and algorithms. " O'Reilly Media, Inc.", 2018.
3. Halder, Soma, and Sinan Ozdemir. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem. Packt Publishing Ltd, 2018.
4. Alessandro Parisi. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd, 2019.

9. Page Web du cours :

http://moodle.uqo.ca