+1 (438) 938-4368
Montréal, Québec H3T 1J4
kacem.khaled@polymtl.ca

Kacem Khaled

Doctorant en intelligence artificielle

sites.google.com/view/kacemkhaled
github.com/kacemkhaled
linkedin.com/in/kacemkhaled

Sommaire

- **Candidat au doctorat en intelligence artificielle**, aspirant scientifique de données passionné par la résolution de problèmes avec des compétences pratiques dans le développement de modèles d'apprentissage automatique et une expérience internationale en ingénierie des systèmes embarqués. Demande d'adhésion à l'OIQ en cours ;
- **Expérience en apprentissage automatique et en apprentissage profond** : développement et validation de modèles d'apprentissage automatique et d'apprentissage profond pour le traitement du langage naturel et les tâches de vision ;
- **Compétence en science des données** : recherche, collecte et nettoyage de données, visualisation et analyse de données ;
- **Qualités professionnelles:** esprit analytique, soucieux du détail et rigoureux. Solides compétences en communication bilingue, qui me permettent de vulgariser efficacement les concepts liés à l'apprentissage automatique lors des présentations.

Études

Candidat au doctorat, Génie informatique - Intelligence artificielle, GPA : 4,0/4,0 **09/2019 — (prévu) 08/2024**
Polytechnique Montréal, Université de Montréal *Montréal, QC*
Directrice de recherche : Prof. Gabriela Nicolescu
Projet de recherche du CRSNG en collaboration avec Synopsys Inc. : Ma recherche doctorale porte sur la robustesse des algorithmes d'apprentissage automatique. Je m'intéresse à l'amélioration de leur fiabilité et à leur protection contre les attaques adversariales.

Diplôme national d'ingénieur, Informatique industrielle et automatique, GPA : 3,7/4,0 **09/2014 — 07/2019**
Équivalence au Canada: Baccalauréat et Maîtrise, lien vers la badge d'équivalence WES Canada (World Education Services)
Institut National des Sciences Appliquées et de la Technologie (INSAT), Université de Carthage *Tunis, Tunisie*

Expérience professionnelle

Doctorant Scientifique en IA appliquée / Développeur en apprentissage automatique (ML) **09/2019 — Présent**
Polytechnique Montréal, en collaboration avec Synopsys Inc. *Montréal, QC*

- Collaborer avec les parties prenantes pour comprendre les besoins de l'entreprise et aligner les solutions d'IA/ML sur les objectifs de l'organisation.
- Développer et mettre en oeuvre des modèles de l'état de l'art en aprentissage profonds sur des système de calcul de haute performance (HPC).
- Améliorer la robustesse des modèles d'apprentissage profond contre les attaques adversarialles, notamment les attaques d'extraction.

Stagiaire en génie logiciel embarqué **02/2019 — 07/2019 & 08/2018 — 09/2018**
German Autolabs GmbH, Startup technologique, développant un assistant virtuel pour les automobilistes. *Berlin, Allemagne*

- Concevoir et mettre en œuvre un algorithme de formation de faisceau pour la capture audio à partir d'une direction spatiale donnée à l'aide d'un réseau de microphones circulaires. Ce projet fait partie du PoC en vue d'une éventuelle mise en œuvre future dans un assistant numérique pour les automobilistes.
- Participer à l'effort de développement du micrologiciel, écrire le code de production et les fonctionnalités grand public.
- Collaborer avec l'équipe d'ingénieurs pour améliorer le micrologiciel responsable du traitement audio au sein d'un pipeline d'assistant virtuel.

Stagiaire en ingénierie des systèmes embarqués **07/2018**
Volatiles Lighting GmbH, Startup technologique, développant des carreaux tactiles et lumineux pour décoration luxueuse. *Berlin, Allemagne*

- Contribuer à la conception d'un prototype pour une génération moins coûteuse de "volatiles" (R&D, proposition d'une nouvelle solution matérielle, conception de circuits imprimés, évaluation de nouveaux circuits intégrés et développement d'un pilote au niveau du micrologiciel).

Expérience en enseignement

Chargé de cours / *Cours INF1005D : Programmation procédurale en Python* **Hivers 2022/2023/2024 & Automnes 2021/2022/2023**
Polytechnique Montréal, *Responsable du cours : Prof. Martine Bellaïche* *Montréal, QC*

Chargé des travaux pratiques / *Cours INF8225 : Intelligence artificielle* **Hivers 2021/2023**
Polytechnique Montréal, *Responsable du cours : Prof. Christopher Pal* *Montréal, QC*

Chargé de laboratoire, Répétiteur / *Cours INF1500 : Logique des systèmes numériques* **Hivers 2020/2021 & Automnes 2020/2022**
Polytechnique Montréal, *Responsables du cours : Prof. Sylvain Martel et Prof. Gabriela Nicolescu* *Montréal, QC*

Compétences

Développement:	Python, C, C++, SQL, VHDL
Cours universitaires:	Intelligence artificielle, apprentissage profond, fouille de données, traitement automatique des langages naturels, algorithmes et structures de données, communication scientifique et technique
Cours en ligne certifiés:	Spécialisation en apprentissage profond, enseignée par : Prof. Andrew Ng sur Coursera [Certificats]
Technologies / Outils:	Git, PyTorch, PyTorch Lightning, TensorFlow, Keras, Spark, Scikit-Learn, Pandas, WandB, Tensorboard
Méthodologies:	Agile, Scrum, Kanban
Langues:	Français (courant), Anglais (courant), Allemand (élémentaire)

+1 (438) 938-4368
Montréal, Québec H3T 1J4
kacem.khaled@polymtl.ca

Kacem Khaled

Doctorant en intelligence artificielle

sites.google.com/view/kacemkhaled
github.com/kacemkhaled
linkedin.com/in/kacemkhaled

Projets sélectionnés

Cadre d'extraction pour les modèles d'apprentissage profond, lien du project sur github *Montréal, QC* | Automne 2021 - Été 2022
Travail de doctorat au laboratoire HES, Polytechnique Montréal
Un cadre pour l'évaluation de la vulnérabilité des attaques de vol de modèle contre les modèles d'apprentissage profond entraînés de façon adversariale. Mots clés : Pytorch, Pytorch Lightning, WandB, Deep Learning, Confidentialité, Robustesse

Analyse des réseaux sociaux, lien de projet sur github *Montréal, QC* | Été 2020
Projet universitaire dans le cadre du cours INF8111 Fouille des données

- Implémenter l'algorithme LPAm+ pour détecter les communautés parmi les personnages de Games of Thrones.
- Analyser le réseau social pour trouver les personnes les plus influentes dans le réseau.

Mots-clés : Python, Clustering, Graphs.

Analyse du panier de marché (Market Basket Analysis), lien du projet sur github *Montréal, QC* | Été 2020
Projet universitaire dans le cadre du cours INF8111 Fouille des données

- Développer un algorithme d'analyse du panier de marché pour révéler les habitudes d'achat dans l'ensemble de données Instacart avec plus de trois millions de transactions de supermarchés.
- Analyser les informations commerciales sur les tendances des clients, par exemple sur les produits les plus achetés qui ont la plus forte probabilité d'être commandés à nouveau.

Mots-clés : Python, Google Cloud Platform, Spark, SQL, Matplotlib, Data Science, Data Mining, Map-Reduce.

Système de recommandation pour un site web Q&A, lien du projet sur github *Montréal, QC* | Été 2020
Projet universitaire dans le cadre du cours INF8111 Data Mining

- Développer un système de recommandation qui renvoie les fils de discussion (questions + réponses) qui sont liés à une question spécifique.

Mots-clés : Python, NLTK, Scipy, Scikit-Learn, Traitement du langage naturel.

Robots autonomes, lien vers mon portfolio *La Roche-sur-Yon, France* | *Paris, France* | *Tunis, Tunisie* | Automne 2015 – Été 2017
Projets extrascolaires au sein d'un club de robotique universitaire (AeRobotix INSAT)
Participation au développement de robots mobiles autonomes qui obéissent à des spécifications uniques de défis robotiques : Eurobot / Tunirobots. Des équipes de 6 à 8 élèves ingénieurs développant deux robots par concours : Eurobot 2017 (La Roche-sur-Yon, France), Eurobot 2016 (Paris, France), Tunirobots 2016 (Tunis, Tunisie). Mots-clés : Python, C++, STM32, Raspberry Pi, SolidWorks, PCB Design, Electronics.

Publications Scientifiques

- **Khaled, K.**, Dhaoudi, M., Nicolescu, G., De Magalhães, F. G. (2023). Efficient Defense Against Model Stealing Attacks on Convolutional Neural Networks. In 2023 22nd IEEE International Conference on Machine Learning and Applications (ICMLA). Lien ArXiv.
- **Khaled, K.**, Nicolescu, G., De Magalhães, F. G. (2022, August). Careful What You Wish For: on the Extraction of Adversarially Trained Models. In 2022 19th Annual International Conference on Privacy, Security Trust (PST) (pp. 1-10). IEEE., doi : 10.1109/PST55820.2022.9851981.
- Raj, A. S., Tenison, I., **Khaled, K.**, de Magalhães, F. G., Nicolescu, G. FedSHIBU: Federated Similarity-based Head Independent Body Update. In Workshop on Federated Learning: Recent Advances and New Challenges, in Conjunction with NeurIPS 2022 (FL-NeurIPS'22). Lien OpenReview.

Activités sociales

Gagnant du 1er prix au hackathon CodeML 2023 hackathon dans le concours de détection d'émotions *Montréal, QC* | 10/2023
Bénévole à CABBC (Centre d'action bénévole de Bordeaux-Cartierville) *Montréal, QC* | 2023
Membre de Calculum (Club de programmation compétitive de l'Université de Montréal) *Montréal, QC* | 2022/2023
Membre de Dirobots (Club de robotique exploitant l'apprentissage par renforcement à l'Université de Montréal) *Montréal QC* | 2022/2023
Participant au hackathon CodeML 2022 hackathon (notre équipe a résolu 4/6 défis ML, classée 3ème dans un) *Montréal, QC* | 10/2022
Membre de PolySTAR (Club de robotique à Polytechnique Montréal) *Montréal, QC* | Hiver 2020
Membre du comité de Association des techniques de robotique (à distance depuis 2019) *Tunis, Tunisie* | 2016 — 2020
Mentor, responsable R&D et membre de AeRobotix INSAT (club de robotique et d'aéronautique, +200 membres) *Tunis, Tunisie* | 2015 — 2019

Informations personnelles

Intérêts et loisirs: Soccer, Kickboxing, Taekwondo, robotique, jeux vidéos, voyages.

Références

- **Gabriela Nicolescu, Ing., Ph.D.,** Lien : *Directrice de recherche, HES Lab*
  Directrice de département, Professeure titulaire, *Département de génie informatique et de génie logiciel*, Polytechnique Montréal
- **Felipe Gohring de Magalhães, Ph.D.,** Lien : *Collaborateur au laboratoire de recherche HES*
  Associé de recherche, *Département de génie informatique et de génie logiciel*, Polytechnique Montréal
- **Martine Bellaïche, Ph.D.,** Lien : *Responsable d'un cours où j'étais chargé de cours*
  Professeure titulaire, *Département de génie informatique et de génie logiciel*, Polytechnique Montréal