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

Kacem Khaled

PhD Candidate in Artificial Intelligence

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

Summary

- **PhD Candidate in Artificial intelligence**, aspiring Data Scientist passionate about problem-solving with hands-on skills in developing machine learning models and international engineering experience in embedded systems and hardware. OIQ membership application in progress;
- **Experience in machine learning and deep learning**: development and validation of machine learning and deep learning models for natural language processing and vision tasks;
- **Data science skills:** research, collection and cleaning of data, data visualization and analysis;
- **Professional qualities:** Analytical, detail-oriented and rigorous mind. Strong bilingual communication skills, which allow me to effectively popularize concepts relating to machine learning during presentations to stakeholders;
- I am seeking a part-time job or internship in Data Science or Machine Learning. I am open to working in Montreal, or remotely.

Education

PhD Candidate, Computer Engineering – Artificial Intelligence, GPA: 4.0 **SEP 2019 – Expected AUG 2024**
Polytechnique Montreal – Department of Computer Engineering and Software Engineering *Montreal, QC*

- Advisor: Prof. Gabriela Nicolescu, Research Lab: Heteregenous Embedded Systems (HES)
- My thesis is about the robustness and the privacy of machine learning algorithms. My research focuses on improving their robustness and protecting them from adversarial attacks. NSERC research project in collaboration with Synopsys Inc. (Ottawa).

National Diploma in Engineering, Industrial Computer Science and Automation Engineering, GPA: 3.69 **SEP 2014 – JUL 2019**
National Institute of Applied Sciences and Technology (INSAT), University of Carthage *Tunis, Tunisia*

- Equivalency in Canada: Bachelor's and master's degree, link to the WES (World Education Services) equivalency badge.

Professional Experience

Researcher / Deep Learning **SEP 2019 — Present**
Polytechnique Montreal, in collaboration with Synopsys Inc. *Montreal, QC*

- NSERC Research Project: Risk Assessment and Mitigation of Deep Learning Model Extraction Attacks in Neural Network Accelerators

Embedded Software Engineering Intern **FEB — JUL 2019 / AUG — SEP 2018**
German Autolabs GmbH, Technology Company, building digital assistant for drivers *Berlin, Germany*

- Design and implement a beamforming algorithm for audio capture from a given spatial direction using a circular microphone array. This project is part of PoC for a possible future implementation in a digital assistant for drivers.
- Participate in the firmware development effort, write production code and consumer features.

Hardware Engineering Intern **JUL 2018**
Volatiles Lighting GmbH, Lighting Technology Company, developing smart surface light solutions *Berlin, Germany*

- Contribute to the design of a prototype for a lower-cost generation of the "volatiles" (R&D, Propose of a new hardware solution, PCB Design, Prototype, Evaluate new ICs and firmware level driver development).

Teaching Experience

Lecturer / Course INF1005D: Python Programming **Fall 2023 / Winter 2023 / Fall 2022 / Winter 2022 / Fall 2021**
Polytechnique Montreal, *course coordinator: Prof. Martine Bellaïche* Montreal, QC

Teaching assistant / Course INF8225: Artificial Intelligence: probabilistic and learning techniques **Winter 2023 / Winter 2021**
Polytechnique Montreal, *course coordinator and instructor: Prof. Christopher Pal* Montreal, QC

Teaching assistant / Course INF1500: Logic of digital systems **Fall 2022 / Winter 2021 / Fall 2020 / Winter 2020**
Polytechnique Montreal, *course coordinators and instructors: Prof. Sylvain Martel and Prof. Gabriela Nicolescu* Montreal, QC

Skills

Development:	Python, SQL, C, C++, Matlab, VHDL
University courses:	Artificial Intelligence, Deep Learning, Data Mining, Natural Language Processing, Algorithms and Data Structures, Databases, Scientific and Technical Communication
Certifications:	Deep Learning Specialization, *taught by: Prof. Andrew Ng on Coursera*, includes 5 certified courses: Improving Deep Neural Networks, Structuring Machine Learning Projects, Sequence Models, Convolutional Neural Networks, Neural Networks and Deep Learning. Link to Certificate
Technologies / Tools:	Git, PyTorch, PyTorch Lightning, TensorFlow, Keras, Spark, Scikit-Learn, Pandas, WandB, Tensorboard
Methodologies:	Agile, Scrum, Kanban

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

Kacem Khaled

PhD Candidate in Artificial Intelligence

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

Selected Projects in Machine Learning and Data Science

Extraction framework for deep learning models, project link on github — *Montreal, QC* | Fall 2021 – Summer 2022
PhD work at HES Lab, Polytechnique Montreal
A Framework for vulnerability assessment of model stealing attacks against adversarially trained Deep Learning models.
Keywords: Pytorch, Pytorch Lightning, WandB, Deep Learning, Privacy, Robustness

Social Network Analysis, project link on github — *Montreal, QC* | Summer 2020
University project within the course INF8111 Data Mining

- Implement the LPAm+ algorithm to detect the communities among the characters of Games of Thrones.
- Analyze the social network to find the most influential people in the network.

Keywords: Python, Clustering, Graphs.

Market Basket Analysis, project link on github — *Montreal, QC* | Summer 2020
University project within the course INF8111 Data Mining

- Develop a Market Basket Analysis algorithm for revealing purchase patterns in the Instacart dataset with more than three million supermarket transactions.
- Analyze Business Insights about customer trends e.g. about the top purchased products with the highest probability of being reordered.

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

Recommendation System for a Q&A website, project link on github — *Montreal, QC* | Summer 2020
University project within the course INF8111 Data Mining

- Develop a recommendation system that returns threads (question + answers) that are related to a specific question.

Keywords: Python, NLTK, Scipy, Scikit-Learn, Natural Language Processing.

Social activities

Volunteer at CABBC (Centre d'action bénévole de Bordeaux-Cartierville) — *Montreal, QC* | 2023
Member at Calculum (Competitive Programming Club at the University of Montreal) — *Montreal, QC* | 2022/2023
Member at Dirobots (Robotics club using reinforcement learning at the University of Montreal) — *Montreal, QC* | 2022/2023
Participant at in CodeML 2022 hackathon (we solved 4/6 ML challenges, we ranked 3rd in one) — *Montreal, QC* | OCT 2022
Member at PolySTAR (Robotics Club at Polytechnique Montreal) — *Montreal, QC* | Winter 2020
Board Member at Association of Robotics Techniques (remotely since 2019) — *Tunis, Tunisia* | DEC 2016 – DEC 2020
Mentor, R&D Manager and Member at AeRobotix INSAT (robotics and aeronautics club, +200 members) — *Tunis, Tunisia* | SEP 2015 – JAN 2019
Member at IEEE INSAT Student Branch (Region 8) (Robotics Automation Society Chapter) — *Tunis, Tunisia* | MAR 2018 – JAN 2019

Personal information

Languages: English (fluent), French (fluent), German (elementary)
Interest and hobbies: Soccer, Kickboxing, Taekwondo, robots, video games, trips, cooking.

Publications

- **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). ArXiv link*
- **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). ArXiv link*
- 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).*

References

- **Gabriela Nicolescu, Dr.,** — Relationship: *Current advisor, HES Lab*
  Department Director, Full Professor, *Department of Computer Engineering and Software Engineering*
  Polytechnique Montreal, University of Montreal
- **Felipe Gohring de Magalhães, Ph.D.,** — Relationship: *Collaborator at HES Lab*
  Research Professional, *Department of Computer Engineering and Software Engineering*
  Polytechnique Montreal, University of Montreal
- **Martine Bellaïche, Ph.D.,** — Relationship: *Coordinator of a course where I serve as a Lecturer*
  Full Professor, *Department of Computer Engineering and Software Engineering*
  Polytechnique Montreal, University of Montreal