+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

Affiliation:
Heteregenous Embedded Systems (HES) – Office M-4208, Department of Computer Engineering and Software Engineering, Polytechnique Montreal, University of Montreal
Research interests:
Deep learning, machine learning privacy and security, computer vision, natural language processing, model compression.

Education

PhD Candidate, Computer Engineering – Artificial Intelligence, GPA: 4.0 **SEP 2019 – Expected AUG 2024**
Polytechnique Montreal, University of Montreal *Montreal, QC*
Advisor: Prof. Gabriela Nicolescu
NSERC research project in collaboration with Synopsys Inc.: My doctoral research is about the privacy and the security of machine learning algorithms. My interests focus on improving their robustness and protecting them from malicious attacks.

National Diploma in Engineering, Industrial Computer Science and Automation Engineering, GPA: 3.69 **SEP 2014 – JUL 2019**
Equivalency in Canada: Bachelor's and master's degree, link to the WES (World Education Services) equivalency badge
National Institute of Applied Sciences and Technology (INSAT), University of Carthage *Tunis, Tunisia*

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 implementation of 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.
- Participation in the firmware development effort, writing production code and consumer features.

Hardware Engineering Intern **JUL 2018**
Volatiles Lighting GmbH, Lighting Technology Company, developing smart surface light solutions *Berlin, Germany*
- Contribution to the design of a prototype for a lower-cost generation of the "volatiles" (R&D, Proposition of a new hardware solution, PCB Design, Prototyping, Evaluation of new ICs and firmware level driver development).

Engineering Intern (part-time) **FEB - MAY 2018**
Peaksource, Technology Company specialized in IT, Pro-Events and Digital Marketing *Tunis, Tunisia*
- Development of applications based on microcontrollers and dedicated to Digital Marketing projects (R&D, Python/C++ Programming, PCB Design, Electronics, Prototyping).

Engineering Intern **JUL 2017**
Cement Company of Gabes - Secil Group, Industrial company that mainly manufactures Cement *Gabes, Tunisia*
- Development of a PoC of replacing of a PLC by a microcontroller for the control of the industrial aspirator (R&D, Electronics, C Programming).

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

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).*

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, IEEE Xplore 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).*

+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

Projects

Extraction framework for deep learning models, project link on github — *Montreal, QC* | Fall 2021 – Summer 2022
A Framework for vulnerability assessment of model stealing attacks against adversarially trained Deep Learning models.
Technologies: Pytorch, Pytorch Lightning, WandB

Autonomous Robots — *Tunis, Tunisia* | Fall 2015 – Summer 2017
Extracurricular projects within a university robotics club (AeRobotix INSAT)
Participation in the development of mobile autonomous robots that obey unique specifications of robotic constests: Eurobot / Tunirobots. Teams of 6-8 engineering students developing two robots per contest: Eurobot 2017 (La Roche-sur-Yon, France), Eurobot 2016 (Paris, France), Tunirobots 2016 (Tunis, Tunisia)

Academic community service

Student speaker at Cyber conference 2021 — *Montreal, QC (virtual)* | Spring 2021
External reviewer (Paper) at DAC 2021 (The 58th Design Automation Conference) — Winter 2021
Student Volunteer at FPS 2020 (the 13th International Symposium on Foundations Practice of Security) — *Montreal, QC (virtual)* | Fall 2020
Student Volunteer at FETCH 2020 (Winter Workshop on Heterogeneous Embedded Systems Design Technologies) — *Montreal, QC* | Winter 2020

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

Skills

Development: Python, C, C++, Matlab, VHDL
University courses: Artificial Intelligence, Deep Learning, Data Mining, Natural Language Processing, Algorithms and Data Structures, Scientific and Technical Communication
Certified online courses: Deep Learning Specialization, taught by: Prof. Andrew Ng on Coursera Link to Certificate
Technologies / Tools: Git, PyTorch, PyTorch Lightning, TensorFlow, Keras, Spark, Scikit-Learn, WandB, Tensorboard

Personal information

Languages: English (fluent), French (fluent), German (elementary), Arabic (native)
Interest and hobbies: Practising sports: Soccer, Kickboxing, former black belt athlete of Taekwondo (since 2013), building robots, playing video games, travelling, cooking.

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
- **Christopher J. Pal, Ph.D.,** Relationship: *Coordinator and instructor of a course where I serve as a Teaching assistant*
  Full Professor and Canada CIFAR AI Chair, *Department of Computer Engineering and Software Engineering*
  Polytechnique Montreal, University of Montreal