Amr M. Saber

PhD Candidate, University of Toronto, Toronto, Ontario, Canada
amr.mohamedsab@gmail.com | +1(416)294-0018 | linkedin.com/in/amrmsaber | github.com/amrmsab

SUMMARY

AI researcher – highly passionate about safe deployment of AI systems – with 5+ years of experience pioneering deep learning solutions to improve safe decision-making for autonomous systems. 10+ of proficiency in Python, with expertise in various ML frameworks, including PyTorch and TensorFlow. Expertise developing safe AI solutions for safety-critical infrastructure, including the electric grid, and autonomous vehicles.

EDUCATION

University of Toronto, Division of Applied Science and Engineering

- **PhD**, Electrical and Computer Engineering — Sep. 2020 — Jun. 2024
  - GPA: 4.0/4.0. Ontario Graduate Scholar. A.G. Bell Canada Graduate Scholar. E.S. Rogers Sr. Fellow.
  - Research topic: Artificial intelligence (AI) for cyber-physical security.
- **MASc**, Electrical and Computer Engineering — Sep. 2018 — Jun. 2020
  - GPA: 4.0/4.0. Hatchery Entrepreneurial Fellow. E.S. Rogers Sr. Fellow.
  - Research topic: Enhancing electric grid cyber-resilience.
- **BASc**, Engineering Science — Sep. 2012 — Jun. 2017
  - Major GPA: 3.97/4.0. Minor in Business. Honor's Graduate.
  - Research topic: Data-driven decision making for demand response in the electric grid.

EXPERIENCE

Teaching Fellow
University of Toronto, Toronto & Queen's University, Kingston, Ontario, Canada — Jan. 2019 — May 2023

- Developing a new course on computer vision for autonomous vehicles. Instructing 250 students in key tools, including Python, OpenCV, ROS, Docker, Git, and UNIX. Mentoring students on AI ethical considerations.
- Instructed a senior capstone course, facilitating student engagement with industry clients in healthcare, tech, and finance. Recruited 15+ projects from 10+ clients, and secured $500 in funding for each team. Coached students on client-relationship management, engineering design, and project management.
- Instructed a senior control systems course for 50 engineering students. Introduced students to dynamical system modelling, MATLAB, Simulink, and PID control design.
- Contributed to the development of 4 courses and served as a teaching assistant for 7 different courses spanning machine learning, signals and systems, probability and statistics. Received 20+ teaching award nominations.

Research Scientist, PhD — Sept. 2018 — Present
University of Toronto, Toronto, Ontario, Canada

- Designed and led 3 innovative research projects leveraging AI for cybersecurity, involving the use of deep reinforcement learning (RL), safe RL, and real-time threat response using various neural networks (e.g., variational autoencoders, RNN/LSTM, CNN-based classifiers, and GANs).
- Supervised and mentored 3 students in their theses, providing guidance on research methodologies and AI tools.
- Integrated power system analysis and deep learning libraries in Python, including OpenAI Gym, Stable Baselines, and Pandapower. Contributed to the open-source Pandapower project.
- Contributed research enhancing threat response precision by up to 30% over the state-of-the-art. Presented research findings at multiple conferences.

Electrical Engineering Intern (EIT) — Jul. 2017 — Sep. 2018
Hatch - Consulting Firm, Mississauga, Ontario, Canada

- Led engineering design for equipment upgrades at the largest gold mine in the Americas, producing 150+ drawings, layouts, calculations, cost and quantity estimates in compliance with safety codes, resulting in 4× increase in process reliability and a 2× in production capacity.
- Supervised on-field project commissioning and troubleshooting, managing a team of 30+ technicians, ensuring safety compliance, and receiving commendation for timely project delivery.

- Conducted load flow, contingency, fault analysis, and motor studies for a new 30 megawatt substation in Asia.
- Performed feasibility and technical reviews for cutting-edge technologies developed by startups to enhance operational efficiency in mining operations.

Data Analyst May. 2015 — Jan. 2016
Ontario Electricity System Operator (IESO), Oakville, Ontario, Canada

- Spearheaded 3 data analytics and visualization tools utilizing Visual Basic, SQL, and Python to distill electricity market data into actionable insight and key trends for organizational leadership.
- Streamlined data processing for faster results by implementing advanced analytics tools. Introduced Tableau within the division, demonstrating the application of modern data tools to create visual narratives highlighting emerging market trends.
- Investigated and recovered CAD $1M of excessive market payments, conducting in-depth market data analysis to ensure compliance with market rules and identify areas for rules improvement.

SKILLS

- **Programming Languages:** Proficient in Python, MATLAB. Experience with C, C++, Julia, R, SQL, VBA. Familiar with Go, Java.
- **Data Science Tools:** Proficient with Pandas, Numpy, SciPy, Matplotlib, Seaborn, Plotly.
- **Machine Learning Frameworks:** Proficient with PyTorch, Scikit-Learn, OpenAI Gym, RLib, StableBaselines, OpenCV. Experience with TensorFlow, Keras, NLTK.
- **Cloud Platforms:** Experience with AWS
- **Technologies**: Experience with Git, GitHub, Docker. Familiar with Spark.
- **Domain-specific Knowledge**: Expertise in Computer Vision, Autonomous Systems, Reinforcement Learning, Robotics, Optimization, Linear Algebra, Probability and Statistics.

Relevant Coursework: Machine Learning (CSC2515) (A+). Probabilistic Learning and Reasoning (CSC2505) (A+). Data Science and Analytics (MIE1624) (A). Convex Optimization (ECE1505) (A).

SELECT PUBLICATIONS

- **A. S. Mohamed** and D. Kundur. "Engaging Cyberattackers in Cyber-physical System Honeypots" Submitted: IEEE Transactions of Smart Grid. ID: TSG-01882-2023
- **A. S. Mohamed** and D. Kundur, "Safe Reinforcement Learning-based Automatic Generation Control" Submitted: 2024 IEEE Power & Energy Society General Meeting (PESGM)
- **A. S. Mohamed** and D. Kundur. "On the Use of Reinforcement Learning for Attacking and Defending Load Frequency Control." arXiv preprint arXiv:2303.15736 (2023). Accepted: IEEE Transactions of Smart Grid. ID: TSG-00440-2023
- **A. S. Mohamed**, D. Kundur and M. Khalaf. "A Probabilistic Approach to Adaptive Protection in the Smart Grid." arXiv preprint arXiv:2302.14126 (2023). In review: ACM Transactions on Cyber-physical Systems, ID: TCPS-2023-0016
- **A. S. Mohamed**, S. Lee and D. Kundur, "Reinforcement Learning for Supply Chain Attacks Against Frequency and Voltage Control. arXiv preprint arXiv:2309.05814. Accepted: IEEE International Conference on Machine Learning and Applications 2023.
- **A. S. Mohamed**, M. Khalaf and D. Kundur, "On the Use of Safety Critical Control for Cyber-Physical Security in the Smart Grid," 2023 IEEE Power & Energy Society General Meeting (PESGM), Orlando, FL, USA, 2023, pp. 1-5, doi: 10.1109/PESGM52003.2023.10252487.
- **A. S. Mohamed**, M. F. M. Arani, A. A. Jahromi and D. Kundur, "False Data Injection Attacks Against Synchronization Systems in Microgrids," in IEEE Transactions on Smart Grid, vol. 12, no. 5, pp. 4471-4483, Sept. 2021, doi: 10.1109/TSG.2021.3080693.
- **A. S. Mohamed**, A. Lesage-Landry and J. A. Taylor, "Dispatching thermostatically controlled loads for frequency regulation using adversarial multi-armed bandits," 2017 IEEE Electrical Power and Energy Conference (EPEC), Saskatoon, SK, Canada, 2017, pp. 1-6, doi: 10.1109/EPEC.2017.8286168.