Curriculum Vitæ

Sierra Wyllie

December 13, 2024

Personal Information

Contact:
sierra [at] wyllie.net
sierra.wyllie [at] mail.utoronto.ca
Website: www.syntelliga.net
GitHub: https://github.com/scwyllie
Google Scholar: https://scholar.google.com/citations?user=BFxmLS8AAAAJ&hl=en
LinkedIn: https://www.linkedin.com/in/sierra-wyllie/

Citizenship:
Canada and USA

Education

2020 - 2025	University of Toronto, Engineering Science (BASc), includes one co-op year taken at the Vector Institute
2018 - 2020	Western Kentucky University, Gatton Academy (HS Diploma). Public dual-enrolment program.
2016 - 2020	Henry Clay High School (HS Diploma)

Professional Experience

May 2021 -	**University of Toronto, Vector Institute** Research Intern at the CleverHans Lab with Prof. Nicolas Papernot. Toronto, ON, Canada.
May - Aug. 2024	**EPFL** Research Intern at the SPRING Lab with Prof. Carmela Troncoso. Lausanne, Switzerland.
May - Sept. 2022	**OECD.AI** Technical-focus intern at the Organisation for Economic Co-operation and Development expert group on AI Compute and Climate. Paris, France.
June - Aug. 2020	**Space Tango** Electrical Engineering Intern. Lexington, KY, USA.
May - Aug. 2019	**Western Kentucky University** Undergraduate Researcher in Computer Science. Bowling Green, KY, USA.

Publications

Peer-Reviewed

[1] N. Jia, S. Wyllie, A. Sediq, A. Ibrahim, and N. Papernot, "Backdoor detection through replicated execution of outsourced training," in *3rd IEEE Conference on Secure and Trustworthy Machine Learning*, ser. IEEE SaTML'25. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, 2024.

[2] S. Wyllie, I. Shumailov, and N. Papernot, "Fairness feedback loops: Training on synthetic data amplifies bias," in *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, ser. FAccT '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 2113–2147, note: Work included in the New York Times article "When A.I.'s Output Is a Threat to A.I. Itself" by Aatish Bhatia on Aug. 25, 2024. [Online]. Available: https://doi.org/10.1145/3630106.3659029

[3] A. S. Shamsabadi, S. C. Wyllie, N. Franzese, N. Dullerud, S. Gambs, N. Papernot, X. Wang, and A. Weller, "Confidential-PROFITT: Confidential PROof of fair training of trees," in *International Conference on Learning Representations*, 2023, notable top 5%. [Online]. Available: https://openreview.net/forum?id=iIfDQVyuFD

[4] A. Shahin Shamsabadi, M. Yaghini, N. Dullerud, S. Wyllie, U. Aïvodji, A. Alaagib, S. Gambs, and N. Papernot, "Washing the unwashable : On the (im)possibility of fairwashing detection," in *The Thirty-Sixth Conference on Neural Information Processing Systems (NeurIPS)*, New Orleans, Louisiana, USA,

November 2022. [Online]. Available: https://papers.nips.cc/paper_files/paper/2022/hash/5b84864ff8474fd742c66f219b2eaac1-Abstract-Conference.html

[5] A. White, P. O'Boyle, S. Wyllie, and M. Galloway, "The impact of ddos attacks on application containers, system containers, and virtual machines," in *17th International Conference on Information Technology–New Generations (ITNG 2020)*, S. Latifi, Ed. Cham: Springer International Publishing, 2020, pp. 153–161. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-43020-7_21

Other

1. Contributed to "A blueprint for building national compute capacity for artificial intelligence" by the OECD policy observatory during my internship there. Paper URL.

2. Guest-wrote an article on SaTML'24 for the Schwartz Reisman Institute for Technology and Society (SRI) news section. The article features my own photographs! Link here.

Professional Recognition

Awards

2023 Top 5% Notable Paper at ICLR for [3].
2020 National Honorable Mention for Aspirations in Computing
National Center for Women in Information Technology
2019 First Place Undergraduate Poster
Association for Computing Machinery Mid-Southeast Conference

Grants

FAccT Travel Grant $1800 USD to support travel and attendance at the seventh annual ACM FAccT (Fairness, Accountability, and Transparency) Conference in Rio de Janerio, Brazil from June 3rd-6th. Presented [2].

NSERC USRA $7500 CAD from May-August 2023 from Natural Sciences and Engineering Research Council. Undergraduate Student Research Award given to enable further research in trustworthy machine learning with Prof. Papernot.

ESROP Grant $6000 CAD from May-August 2021 from Engineering Science at the University of Toronto to support research in fairness for machine learning. Work was mentored by Prof. Papernot at the CleverHans trustworthy ML research lab.

Faculty Undergraduate Student Engagement Grant $3000 USD from May-August 2019 from the Western Kentucky University for travel and project-related expenses. The grant was for studying machine learning approaches to network intrusion detection in unmanned aerial vehicle security.

Research Internship Grant $1500 USD from May-August 2019 from the Gatton Academy for housing and project-related expenses. The grant was for studying machine learning approaches to network intrusion detection in unmanned aerial vehicle security.

Conference Addresses

2024	**ACM FAccT** (Rio de Janerio, Brazil) Presentation: Fairness feedback loops: Training on synthetic data amplifies bias
2023	Vector Institute Research Symposium (Toronto, ON) Poster: Confidential-PROFITT: Confidential PROof of fair training of trees
2022	**NeurIPS** (New Orleans, LA) Poster: Washing the unwashable : On the (im)possibility of fair-washing detection
2020	Posters-at-the-Capitol (Frankfort, KY) Poster: Multiclass Network Intrusion Detection In Drones Using Machine Learning
2020	Western Kentucky University Student Research Conference Presentation: Multiclass Network Intrusion Detection In Drones Using Machine Learning
2019	Western Kentucky University Student Research Conference Poster: Meta-Heuristic Approaches to Dynamic Load Balancing
2019	Western Kentucky University Mathematics Symposium Presentation: Network Intrusion Detection In Drones Using Machine Learning
2019	ACM Mid-Southeast Conference Poster: Binary Network Intrusion Detection In Drones Using Machine Learning

Invited Talks

2024 **ETHZ - Florian Tramèr**
Fairness feedback loops: Training on synthetic data amplifies bias

2024 **CISPA - Franziska Boenisch and Adam Dziedzic**
Fairness feedback loops: Training on synthetic data amplifies bias

2024 **MPI Tübingen - Moritz Hardt, Celestine Mendler-Dünner, and Rediet Abebe**
Fairness feedback loops: Training on synthetic data amplifies bias

2024 **EPFL - Carmela Troncoso**
Fairness feedback loops: Training on synthetic data amplifies bias

2024 **AWS**
Fairness feedback loops: Training on synthetic data amplifies bias

2024 **Microsoft's Aether Fairness & Inclusiveness**
Fairness feedback loops: Training on synthetic data amplifies bias

2024 **MPI Bochum – Asia Biega**
Fairness feedback loops: Training on synthetic data amplifies bias

Service

Organising

2024 **TEAS'24** Co-Organizer (with Yoyo Liu) for the first Toronto Ethics in AI Symposium, https://torontoethicsai.org/, sponsored by the Vector Institute.

Reviewing and Volunteering

2024 **NAACL'24** Reviewer for Queer in AI Workshop at the North American Chapter of the Association for Computational Linguistics

2024 **SaTML'24** Volunteer for IEEE Secure and Trustworthy ML. Duties included recording sessions and conference photography.

2024 **ICML'24** Reviewer for International Conference on Machine Learning.

2024 **ICLR'24** Reviewer for International Conference on Learning Representations.

2023 **SaTML'23** Reviewer and volunteer for IEEE Secure and Trustworthy ML.

2022 **NeurIPS'23** Reviewer for Neural Information Processing Systems.

References

Available upon request.