Toluwani Samuel Aremu

AI Researcher | Applied Scientist

KEY COMPETENCIES

- **Skills**: Research, Mathematics, Statistics, Machine Learning, Deep Learning, Data Science, Project Management, Programming, Writing.
- **Tools**: Python, VB.Net, PyTorch, Lightning, TensorFlow, Keras, Jax, Scikit-learn, NumPy, Matplotlib, Visual Studio, Visual Studio Code, PyCharm, Jupyter, Latex, Office 365, Google [Docs, Sheets, Slides].
- **Research Interests**: Trustworthy AI, Responsible AI.

EDUCATION

- **Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), UAE**   AUG 2023 – PRESENT
  - Doctor of Philosophy (PhD) in Machine Learning.
  - Research Areas: Robustness in Computer Vision, Responsible AI.
- **Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), UAE**   JAN 2021 – DEC 2022
  - Master of Science (MSc) in Machine Learning.
  - Research Area: Privacy-Preserving ML.
- **University of Ibadan (UI), Nigeria**   MAY 2018 – MAY 2020
  - Master of Science (MSc) in Computer Science.
  - Research Area: Cryptography and Data Security.
- **Adeleke University, Nigeria**   OCT 2012 – JUL 2016
  - Bachelor of Science (BSc) in Computer Science.
  - Courses: Philosophy, Statistics, Mathematics, Operations Research, Numerical Analysis, Digital Logic, Hardware, Programming Languages, etc.

RESEARCH EXPERIENCE

- **PhD Student, MBZUAI, UAE**   AUG 2023 – PRESENT
  - Research Project Areas: Federated Learning, Efficient Private Inference (PI), Adversarial Defense for Vision-Language Models (VLMs), etc.
- **Research Assistant, MBZUAI, UAE**   FEB 2023 – AUG 2023
  - Research projects: Video Action Recognition, AI for Optimized Scholarly Search, Responsible LLM for Mental Health and Climate Change.
- **Applied Science Intern, M42, UAE**   FEB 2023 – APR 2023
  - Streamlined the preprocessing of the NHANES dataset by building an end-to-end pipeline for downloading, retrieving, analyzing, and modeling.
  - Ensured that the pipeline generates a comprehensive TRIPOD report after use.
- **MSc Student (Graduate Research Assistant), MBZUAI, UAE**   JAN 2021 – DEC 2022
  - Developed PolyKervNets to minimize reliance on ReLU activations and optimize latency in AI models during private inference.
  - Projects: Self-Supervised Racial Bias Mitigation in Face Recognition Systems, Accented Speech Recognition using Vector-Quantized Variational AutoEncoders (VQ-VAE), Gender Bias Mitigation in Word Embeddings.

TEACHING EXPERIENCE

- Teaching Assistant, Object Oriented Programming (OOP) [UI, Nigeria]   2019

VOLUNTEERING EXPERIENCE

- Graduate School Application Mentorship   2021 – PRESENT
- Associate Editor, MBZUAI Blog   2024 – PRESENT
- Peer Reviewer
    - IEEE Access   2023
    - Open Information Science   2023
    - NeurIPS   2024
    - ICCTIS   2024

SELECTED PUBLICATIONS

- **Conferences**
    - N. Tastan*, S. Fares*, **T. Aremu***, S. Horvath, and K. Nandakumar, "Redefining Contributions: Shapley-Driven Federated Learning," 33rd International Joint Conference on Artificial Intelligence (IJCAI), Jeju, Korea, 2024.
    - **T. Aremu*** and K. Nandakumar, "PolyKervNets: Activation-free Neural Networks For Efficient Private Inference," *2023 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, Raleigh, NC, USA, 2023, pp. 593-604, doi: 10.1109/SaTML54575.2023.00045.
    - W. Y. Kang*, **T. Aremu***, Y. Balah, M. Nadeem, I. G. Navarette and A. E. Saddik, "ScholarFace: Scanning Faces, Discovering Minds," 2024 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2024, pp. 1-5, doi: 10.1109/ICCE59016.2024.10444350. [Patent Application Submitted]
- **Preprints**
    - S. Fares*, K. Ziu*, **T. Aremu*** *et al.*, "MirrorCheck: Efficient Adversarial Defense for Vision-Language Models," *arXiv.org*, Jun. 13, 2024. https://arxiv.org/abs/2406.09250 (accessed Jun. 20, 2024).
    - **T. Aremu**, "Regularized PolyKervNets: Optimizing Expressiveness and Efficiency for Private Inference in Deep Neural Networks," ePrint IACR, 2023. https://eprint.iacr.org/2023/1917 (accessed Dec. 15, 2023).
    - **T. Aremu** et al., "On the Reliability of Large Language Models to Misinformed and Demographically-Informed Prompts," Jan. 2024, doi: https://doi.org/10.2139/ssrn.4699451.
- **Blog**
    - **T. Aremu**, "Accented Speech Recognition: The Inclusive Realm of Automatic Speech Recognition Systems," Medium, Jul. 03, 2023. https://shorturl.at/oKLP8 (accessed Apr. 27, 2024).
    - **T. Aremu**, "AI Text Detectors: Amazing Sleuths or WHAT?," Medium, Jun. 11, 2023. https://medium.com/towards-artificial-intelligence/ai-text-detectors-amazing-sleuths-or-what-31e4e2ca7803 (accessed Apr. 27, 2024).

SELECTED TALKS & PRESENTATIONS

- Ethical Perspectives of Artificial Intelligence, Department of Material Sciences, University of Denver, Virtual. (JUL 2022).

- PolyKervNets: Activation-free Neural Networks For Efficient Private Inference, IEEE SaTML, North Carolina, USA. (FEB 2023).
- SSIVD-Net: A Novel Salient Super Image Classification and Detection Technique for Weaponized Violence, Computing Conference, London, UK. (JUL 2024).

HONORS & AWARDS

- MBZUAI MSc & PhD Fully Funded Fellowship   2021-2027
- UAE Golden Visa for Talented Persons/Specialists in Science   2022
- MBZUAI Award of Appreciation for Iconic Representation and Student Hospitality 2022
- ProjectSet Innovation Challenge for Entrepreneurship (ICE-22)   2022
- Top 100, DeepLearning.AI Data-Centric AI Competition   2021
- NYSC-FRSC Award for the Most Creative Corp Member   2017
- 2015 AUE-NACOSS Award for the Best Programmer   2015

PROFESSIONAL DEVELOPMENT

- Microsoft Azure
- Deep Learning
- Google Cloud
- IBM AI & Data Science
- Machine Learning
- MLOps
- Mind & AI

REFERENCES

- Prof. Abdulmotaleb El Saddik - Enterprise Professor, MBZUAI & UOttawa - a.elsaddik@mbzuai.ac.ae.
- Prof. Kun Zhang - Professor, MBZUAI & Carnegie Mellon University - kun.zhang@mbzuai.ac.ae.
- Dr. Karthik Nandakumar - Associate Professor, MBZUAI - karthik.nandakumar@mbzuai.ac.ae.