NTUNG NGELA LANDON

Cybersecurity Researcher — AI/ML Security — Trustworthy AI

nngelala@andrew.cmu.edu — landonntung71@gmail.com

linkedin.com/in/ntung-landon — github.com/ntung-landon — ntunglandon-portfolio.vercel.app

RESEARCH PROFILE

Cybersecurity researcher working at the intersection of artificial intelligence and security, with research experience spanning biometric security, machine learning robustness, fairness, and the evaluation of AI-enabled systems. My research began with demographic fairness in face Presentation Attack Detection (PAD), where I investigated how preprocessing, decision thresholds, and model architectures influence demographic disparities. I subsequently extended this work to study the stability of fairness measurements under cross-dataset distribution shift, controlled ablations, and random-seed variation. This trajectory has developed my broader interest in the security, robustness, reliability, and trustworthy deployment of machine learning systems. I have led two published research papers and contributed to two additional manuscripts currently under review.

RESEARCH INTERESTS

AI/ML Security; Adversarial Machine Learning; Security and Robustness of Machine Learning Models; Trustworthy AI; Machine Learning Evaluation; Computer Vision Security; Biometric Security; Face Presentation Attack Detection; Fairness and Responsible AI; Robustness and Generalization; Security of AI-Enabled Authentication Systems.

RESEARCH CONTRIBUTIONS

- **Fairness-aware biometric security:** Developed a lightweight face Presentation Attack Detection (PAD) methodology combining Local Binary Patterns, ethnicity-aware preprocessing, group-specific threshold optimization, and statistical fairness analysis to investigate and reduce demographic disparities.
- **Architecture and demographic bias:** Led a comparative study of convolutional and Vision Transformer architectures to examine the relationship between model architecture, demographic performance disparities, and cross-demographic generalization in face PAD.
- **Robustness and reproducibility of AI evaluation:** Investigated whether fairness measurements obtained from individual training runs remain reliable under cross-dataset distribution shift, controlled ablations, and random-seed replication.
- **Security research methodology:** Applied controlled experimentation, cross-dataset evaluation, multi-seed replication, statistical analysis, and reproducibility-focused evaluation to distinguish genuine model behavior from experimental variability.

EDUCATION

Carnegie Mellon University — Pittsburgh, USA
Master of Science in Information Technology – Cybersecurity — August 2024 – December 2025
GPA: 3.64/4.00

- Final Practicum: *Cross-Platform Automated Malware Analysis Pipeline.*
- Graduate research in AI security, biometric security, machine learning, computer vision, and cybersecurity.

University of Buea — Buea, Cameroon
Bachelor of Engineering in Computer Engineering — October 2019 – June 2023
GPA: 3.51/4.00

- Final-Year Project: *Design and Implementation of a Cognitive-Based IoT Fetal Movement Monitoring System.*

RESEARCH EXPERIENCE

Carnegie Mellon University
Research Associate March 2026 – March 2027

- Lead research investigating the robustness and reproducibility of demographic fairness in face Presentation Attack Detection (PAD) under distribution shift.
- Evaluate a two-branch PAD framework across CASIA-SURF CeFA, OULU-NPU, and SiW-M using Single-Source Generalization (SSG) and Leave-One-Dataset-Out (LODO) protocols.
- Conduct five-seed replication experiments and controlled ablation studies to evaluate the stability of fairness measurements across datasets, architectures, preprocessing configurations, and random seeds.
- Observe stable aggregate discrimination under cross-dataset shift, with mean AUCs of 76.8% for SSG and 76.7% for LODO, while demographic fairness gaps remain substantially larger and less stable.
- Measure a mean best-to-worst treated-group fairness gap of 30.6 percentage points on the ethnicity-labelled CeFA test set across five seeds, with observed gaps ranging from 23 to 39 percentage points.
- Demonstrate that no individual design choice, including the second model branch, multi-source training, or ethnicity-aware preprocessing, produced a statistically significant change in the fairness gap after accounting for seed variance.
- Manuscript: *Fairness Under Distribution Shift in Face Presentation Attack Detection: A Cross-Dataset and Ablation-Based Analysis* (under review).
- Working on a Microsoft-funded cybersecurity research project investigating malware analysis and the robustness of malware detection systems, including the evaluation of malware.
- Conduct controlled malware experimentation and analysis to examine how changes in malware samples affect target systems.

Carnegie Mellon University
Research Assistant August 2025 – December 2025

- Led an empirical investigation into whether model architecture contributes to demographic disparities in face Presentation Attack Detection.
- Designed and implemented comparative experiments evaluating Multimodal ViT-Tiny, ResNet18, and pretrained DeiT-S architectures on the CASIA-SURF CeFA dataset.
- Evaluated models across African, East Asian, and zero-shot Central Asian demographic groups to investigate demographic fairness and cross-demographic generalization.
- Conducted PAD evaluation using accuracy, APCER, BPCER, ACER, and Equal Error Rate (EER).
- Demonstrated that pretrained DeiT-S achieved 97.27% overall accuracy and 0.86% EER, reducing the African–East Asian ACER gap to 0.13%.
- Demonstrated improved zero-shot generalization to Central Asian subjects, with DeiT-S achieving 2.89% BPCER compared with 10.44% for ResNet18.
- Led manuscript development and research interpretation resulting in: *Architectural Bias in Face Presentation Attack Detection: A Comparative Study of Vision Transformers and Convolutional Neural Networks.*

Carnegie Mellon University
Research Intern June 2025 – August 2025

- Initiated research investigating demographic fairness in face Presentation Attack Detection for underrepresented African populations.
- Developed a lightweight PAD pipeline using Local Binary Patterns, ethnicity-aware preprocessing, and group-specific decision threshold optimization.

- Implemented adaptive preprocessing using CLAHE and gamma correction and optimized group-specific decision thresholds using Equal Error Rate minimization.
- Designed fairness evaluation using coefficient of variation, McNemar's statistical testing, and bootstrap confidence intervals.
- Conducted dataset preprocessing, feature extraction, experimentation, validation, visualization, and analysis using CASIA-SURF CeFA.
- Achieved 95.12% accuracy and 98.55% AUC, reducing the African–East Asian accuracy gap from 3.07% to 0.75%.
- Contributed to manuscript development and publication of: *Fairness-Aware Face Presentation Attack Detection Using Local Binary Patterns: Bridging Skin Tone Bias in Biometric Systems.*

RESEARCH PRESENTATIONS

- **"Architectural Bias in Face Presentation Attack Detection: A Comparative Study of Vision Transformers and Convolutional Neural Networks."** Presented at the *10th International Conference on Cryptography, Security and Privacy (CSP 2026)*, Sapporo, Japan, April 2026.

PUBLICATIONS

Peer-Reviewed Journal Publication

1. Jema David Ndibwile, **Ntung Ngela Landon**, and Floride Tuyisenge. "Fairness-Aware Face Presentation Attack Detection Using Local Binary Patterns: Bridging Skin Tone Bias in Biometric Systems." *Journal of Cybersecurity and Privacy*, 6(1), 2026. doi.org/10.3390/jcp6010012.

Conference Paper / Preprint

2. **Ntung Ngela Landon**, Floride Tuyisenge, and Jema David Ndibwile. "Architectural Bias in Face Presentation Attack Detection: A Comparative Study of Vision Transformers and Convolutional Neural Networks." *arXiv:2606.18510*, 2026. doi.org/10.48550/arXiv.2606.18510.

Manuscripts Under Review

3. **Ntung Ngela Landon**, Floride Tuyisenge, Remy Dukundane, Emmanuel Iduh, and Jema David Ndibwile. "Fairness Under Distribution Shift in Face Presentation Attack Detection: A Cross-Dataset and Ablation-Based Analysis." Manuscript under review.
4. Jema David Ndibwile, **Ntung Ngela Landon**, and Lunodzo Mwinuka. "Adversarial Artificial Intelligence Threats in Smart Energy Grids: When Learning Systems Learn from the Attacker." Manuscript under review.

TEACHING EXPERIENCE

Carnegie Mellon University Kigali, Rwanda
Teaching Assistant – CMU Africa Bridge Program January 2025 – April 2025

- Supported undergraduate students preparing for graduate-level study in computing and technology through the CMU Africa Bridge Program.
- Assisted students with technical learning activities, problem solving, and foundational computing concepts required for transition into graduate education.
- Supported instructional delivery, student engagement, academic activities, and student learning.

PROFESSIONAL EXPERIENCE

International Telecommunication Union (ITU), Switzerland
AI, Data Management, and Cybersecurity Intern July 2025 – November 2025

- Conducted hands-on security assessment of an organizational platform using an existing penetration-

testing report as a baseline for further vulnerability investigation.
- Explored the platform to identify additional potential vulnerabilities and security weaknesses.
- Investigated the Digital Object Architecture (DOA) and Advanced Information Management System (AIMS).
- Examined the relationship between artificial intelligence, data management, and data security in AI-enabled information systems.

Reseaux et Telecommunications (Resotel), Cameroon
Networks and Telecommunications Intern September 2022 – February 2023

- Supported installation and initial configuration of surveillance camera systems to strengthen organizational security infrastructure.
- Maintained optical fiber connections to ensure reliable and secure data transmission.
- Deployed a Synology Network Attached Storage (NAS) server to improve secure data storage and accessibility.
- Implemented the 3CX communication platform to improve internal organizational communication.

SELECTED TECHNICAL PROJECTS

Cross-Platform Automated Malware Analysis Pipeline
MSc Final Practicum – Carnegie Mellon University

- Designed and implemented an automated malware-analysis pipeline capable of handling both Windows and Linux malware.
- Integrated CAPE Sandbox with dedicated Windows and Ubuntu virtual machines for controlled malware execution and behavioral analysis.
- Developed an automated workflow that identifies the target operating system of malware samples and routes them to the appropriate analysis environment.
- Connected a honeypot network and malware sample collection to event-hash processing and ingestion scripts feeding the CAPE analysis host.
- Automated analysis and generated structured database reports containing malware-analysis results.
- Integrated the pipeline with the SOC/SIEM of the CMU-Upanzi network to support security monitoring and downstream analysis.

IoT-Based Fetal Health Monitoring System
BEng Final-Year Project – University of Buea

- Designed and implemented an IoT-based system for monitoring fetal movement and health indicators.
- Developed signal-processing algorithms for filtering and analyzing fetal health signals.
- Integrated wireless communication modules for transmitting health data to remote monitoring stations.

RESEARCH METHODS

Experimental Design: Controlled Experiments; Ablation Studies; Cross-Dataset Evaluation; Single-Source Generalization; Leave-One-Dataset-Out Evaluation; Multi-Seed Replication; Reproducibility Analysis.
AI/ML Evaluation: CNNs; Vision Transformers; Transfer Learning; Feature Extraction; Classification; Computer Vision; Model Evaluation; Fairness-Aware Machine Learning.
Biometric Evaluation: APCER; BPCER; ACER; EER; ROC/AUC Analysis; Demographic Performance Gap Analysis.
Statistical Analysis: Bootstrap Confidence Intervals; McNemar's Test; Coefficient of Variation; Statistical Significance Testing.

TECHNICAL SKILLS

Programming & Data: Python; C/C++; JavaScript; NumPy; Pandas; scikit-learn; TensorFlow; OpenCV; Matplotlib.
AI/ML: Computer Vision; Deep Learning; CNNs; Vision Transformers; Transfer Learning; Classification; Feature Extraction; Model Evaluation.
Cybersecurity: Penetration Testing; Ethical Hacking; Vulnerability Assessment; Malware Analysis; Network Security; Wireless Security; Biometric Security; Presentation Attack Detection.
Security Tools: Kali Linux; Wireshark; Burp Suite; Metasploit; Nmap; Nikto; Hydra; CAPE Sandbox.
Systems & Infrastructure: Linux; Windows; Ubuntu; Virtualization; NAS; 3CX; SIEM; Optical Fiber Networks.
Development & Collaboration: Git; GitHub; Arduino IDE.

AWARDS AND HONORS

- **Future Africa Leaders Award**, 2024.
- **Leadership Initiative Award**, 2020.
- **Afretec Inclusion Award**, Women in Tech Club, Carnegie Mellon University.

LEADERSHIP AND SERVICE

Events Manager, Women in Tech Club, Carnegie Mellon University.
Partnership and Sponsorship Lead, Africa Forge Challenge 2.0, Future Africa Leaders Foundation.
Future Africa Leaders Foundation Ambassador.

LANGUAGES

English: Fluent / Native **French:** Intermediate