Philip Akekudaga

Kingston, RI | LinkedIn | (929) 685-9890 | akekulip@gmail.com | GitHub

SUMMARY

Network security researcher with expertise in programmable data planes (P4/Intel Tofino), protocol-level threat detection, traffic measurement, and ML-driven anomaly detection. Builds and evaluates security systems end-to-end—from data plane forwarding logic through automated detection and enforcement. Published 3 IEEE papers on critical infrastructure security with a 4th under review. Strong cross-functional communicator with 8 years of production network infrastructure operations. CompTIA Security+, FAIR, and MITRE ATT&CK certified.

EDUCATION

Ph.D., Electrical Engineering, University of Rhode Island — Jan 2026 – May 2030
- *Research: Programmable Network Security for Critical Infrastructure (P4/SDN, ICS/SCADA, Power Grid)*

M.S., Digital Forensics & Cybersecurity, University at Albany, SUNY – (GPA: 3.9) — Dec 2025

B.Sc., Computer Engineering, KNUST

TECHNICAL SKILLS

Network Programming: P4 (BMv2, Intel Tofino/TNA), P4Runtime, match-action tables, stateful registers, SRAM/TCAM management, SDN/OpenFlow, Mininet

Protocols & Security: TCP/IP, BGP, OSPF, ECMP, DNS, QUIC (familiar), VXLAN/EVPN (familiar), ICS/SCADA, NERC-CIP, IEC 62443, NIST 800-82, NIST CSF/800-53

Measurement & Detection: Splunk (SPL), Microsoft Sentinel (KQL), Wireshark, Scapy, tcpdump, PCAP analysis, flow telemetry, traffic classification, detection engineering

ML/AI: PyTorch (familiar), scikit-learn, GRU/RNN, time-series anomaly detection, feature engineering, AI/LLM prompt engineering

Languages & Tools: Python, C/C++, Bash, SQL, Git, Docker, Linux (daily driver)

RESEARCH EXPERIENCE

CYPHER Lab, University of Rhode Island — Kingston, RI

Research Assistant — Programmable Network Security & Measurement — *Jan 2026 – Present*

- Built adaptive ECMP routing engine in P4 incorporating real-time link utilization telemetry into per-packet path selection, improving throughput balance by 30% and reducing utilization variance by 22% across 4-path topologies (GitHub)
- Developed closed-loop DNS threat defense processing 10K+ packets/sec across 3-hop topologies: telemetry collection, multi-agent reasoning, and dynamic P4Runtime enforcement achieving 97% detection accuracy with <50ms latency (GitHub)
- Implemented stateful DPI pipeline with per-flow tracking across 12 header fields and 5 classification categories; regression suite of 40+ scenarios validates detection across attack variants
- Designed automated measurement framework benchmarking throughput, latency, jitter, and loss across 8+ routing configurations; porting all programs to Intel Tofino hardware (SRAM/TCAM constraints, stage allocation)
- Researching cascading failure risk in power infrastructure using FDNA; paper under review at SmartNets 2026

University at Albany — Innovation Center — Albany, NY

Senior Research Aide (Research Foundation for SUNY) — *Oct 2024 – May 2025*

- Trained GRU model on 500K+ flow records achieving 94% detection accuracy with 18% FP reduction over baseline SVM; engineered 12 features from PCAP-to-dataset pipeline
- Built lightweight ML classifier for edge devices achieving 91% accuracy at 3x lower inference latency; evaluated accuracy-latency tradeoffs across 4 model architectures

INDUSTRY EXPERIENCE

New York State Department of Health — Office of the CISO — Albany, NY

Cybersecurity Analyst Intern — *Aug 2024 – Dec 2025*

- Built Python automation for network security audits across 5,000+ assets via REST APIs, identifying 200+ misconfigurations (60% time reduction); monitored DNS and network telemetry using Splunk/Sentinel; contributed to 15 NIST-aligned security policies

Ghana Water Company LTD. (National Utility — OT/SCADA Environment) — Kumasi, Ghana

IT Officer / MIS Officer — *Sep 2014 – Jan 2022*

- Administered production network infrastructure including SCADA controllers, meters, and ICS network systems for 600+ endpoints across 5 regional sites; 98% patching compliance; automated monitoring with Python/Bash (4 hrs/week saved)

PUBLICATIONS & AWARDS

IEEE UEMCON 2025: Resilient IoT Security: GRU Flood Detection · Privacy-Preserving Lightweight IDS · AI-Enabled Critical Infrastructure Threat Detection

Under Review: Systemic Risk Quantification in Power Infrastructure Using FDNA (SmartNets 2026)

Awards: SIRAcon '25 Research Competition Winner · Cyber 9/12 Strategy Competition Semi-finalist