Priscilla Kyei Danso

Stony Brook University, New York, USA priscillakyeidansoe@gmail.com +1(934)-799-1337

priscilla100.github.io priscilladanso priscilla100

Biography

My research interests lie at the intersection of compliance automation and cybersecurity. I am currently developing ComplianceGPT, a system designed to automate regulatory compliance by integrating formal methods with Large Language Models (LLMs). ComplianceGPT is a hybrid system that combines specialized LLMs with a logic-based compliance checker, translating natural language regulations into First-Order Logic (FOL) formulas using a specialized regulatory vocabulary. Building on my master's research in IoT security, where I applied machine learning models for IoT device profiling, anomaly detection, and vulnerability assessment, I aim to further advance compliance automation and formal verification. I am committed to advancing the state-of-the-art in compliance automation, formal verification, and cybersecurity, contributing to a safer and more resilient digital world.

Education

Stony Brook University, New York, USA *Sept 2023 – Present*
Doctor of Philosophy in Computer Science (PhD)

University of New Brunswick, Fredericton, Canada *May 2021 – May 2023*
Master of Computer Science (MCS)
Thesis: Transferability of Machine Learning Model for IoT device Identification and Vulnerability Assessment.

Kwame Nkrumah University of Science and Technology, Kumasi, Ghana *Sept 2012 – June 2016*
Bachelor of Science in Computer Engineering
Project Title: An Integrated Messaging Platform for an Enterprise Environment

Publications

1. Liam McGevna, Jason Chow, Jeffery Luo, and **Priscilla Kyei Danso**. LLM-Based Anomaly Detection for Digital Substation Cybersecurity (**ACCEPTED**). *2024 IEEE 21st International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, 2024.
2. **Priscilla Kyei Danso**, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Alireza Zohourian, Heather Molyneaux, Rongxing Lu, and Ali A Ghorbani. Transferability of machine learning algorithm for IoT device profiling and identification. *IEEE Internet of Things Journal*, 2024.
3. **Priscilla Kyei Danso**, Euclides Carlos Pinto Neto, Sajjad Dadkhah, Alireza Zohourian, Heather Molyneaux, and Ali A Ghorbani. Ensemble-based intrusion detection for internet of things devices. In *2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, 2022.
4. **Priscilla Kyei Danso**, Heather Molyneaux, Alireza Zohourian, Euclides Carlos Pinto Neto, Derrick Whalen, Sajjad Dadkhah, and Ali A Ghorbani. Human-Centric machine learning: The role of users in the development of IoT device identification and vulnerability assessment. In *HCI for Cybersecurity, Privacy and Trust: 5th International Conference, HCI-CPT 2023, Held as Part of the 25th HCI International Conference, HCII 2023, Copenhagen, Denmark, July 23–28, 2023, Proceedings*
5. Sajjad Dadkhah, Hassan Mahdikhani, **Priscilla Kyei Danso**, Alireza Zohourian, Kevin Anh Truong, and Ali A Ghorbani. Towards the development of a realistic multidimensional IoT profiling dataset. In *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, 2022.
6. Alireza Zohourian, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Hassan Mahdikhani, **Priscilla Kyei Danso**, Heather Molyneaux, and Ali A Ghorbani. IoT zigbee device security: A comprehensive review. *Internet of Things*, 2023.

Research Experience

Graduate Research Assistant *Aug 2023 – Present*
Stony Brook University, New York, USA.

- Conducting an in-depth analysis of LLM capabilities in translating free, unbounded assertive natural language into formal logic expressions.
- Designing experiments to test model effectiveness in identifying logical structures and mapping assertive statements to formal specifications.
- Evaluating and documenting outcomes to refine model capabilities in translating to specific logic forms for applications in compliance and legal reasoning.

Graduate Research Assistant *May 2021 – Dec 2022*

The Canadian Institute for Cybersecurity, Fredericton, Canada

- Engineered a system utilizing machine learning to profile IoT device types within a network while concurrently evaluating and visualizing the vulnerabilities associated with these devices.
- Collaborated with a team to publish an IoT dataset, aiming to facilitate the efforts of researchers specializing in the identification of IoT devices.
- Formulated and executed the implementation of an ensemble-based Intrusion Detection System (IDS), specifically designed for anomaly detection within an IoT infrastructure.
- Conducted extensive research on Internet of Things (IoT) devices, exploring potential vulnerabilities and implementing various efficient mitigation strategies. Executed experiments and thoroughly documented the results.

Technical Skills

Programming: Python, OCaml; **Formal Verification:** NuSMV; **Cybersecurity:** Nmap, Snort; **Research and Technical Writing Skills:** LaTeX, Markdown; **Version Control:** Git, GitHub; **Databases:** MySQL, PostgreSQL