

Md Ajwad Akil

+1 765-543-7512 | ajwadakillabib@gmail.com | [linkedin.com/in/ajwadakil](https://www.linkedin.com/in/ajwadakil) | github.com/AJAkil | ajakil.github.io

BACKGROUND

4th-year Purdue CS PhD student applying ML, LLMs and Agents to security: malware analysis, adversarial malware generation, evasion of ML detectors, and LLM agent security (prompt injection, code hallucination).

EXPERIENCE

Research Engineer Intern

Mountain View, CA

Employer: *Samsung Research America* | *Mobile Platforms and Solutions Lab*

Aug 2026 – Present

- Built an **automated benchmarking** pipeline to evaluate multiple **LLM agents** on **on-device mobile** tasks with real app integrations, comparing agent capability and reliability across LLM backends.
- Conducted **indirect prompt injection (IPI) red-teaming** of on-device mobile agents: designed cross-app attack scenarios and app integrations, then executed **end-to-end attacks** to assess agent robustness.

Machine Learning Engineer Intern

San Francisco, CA

Employer: *DoorDash, Inc.* | *New Verticals, Agentic Catalog*

May 2026 – Aug 2026

- Integrated an in-house **MCP web-search** service into a catalog-enrichment agent, enabling observable multi-round **tool calling**, evidence retrieval, and search-trace capture.
- Built a **multimodal tool-use SFT dataset** via **behavioral distillation** of Gemini search trajectories, then fine-tuned **Qwen3.5 9B/27B VLMs** with **LoRA**, **assistant-only loss masking**, **BF16**, and **multi-GPU DDP** for grounded tool use and attribute extraction.
- Reached **95.5% confirmed precision**; the 27B model exceeded Gemini's attribute coverage by **1.18pp**, stayed within **1.69pp** on precision, and reduced serving-and-search cost by **43%**.

Graduate Research Assistant

West Lafayette, IN

Employer: *Cyber2SLab, Department of Computer Science, Purdue University*

Aug 2023 – Present

- LLMalMorph (Best Paper, IEEE TPS 2025)**: Built a semi-automated pipeline using open-source LLMs and prompt-engineered code transforms to mutate Windows malware source code while preserving functionality and generated **618 variants from 10 samples**, **72%** evasive, with up to **31%** lower AV detection.
- PhantomCall (first author, under submission)**: Built a **black-box attack** that perturbs the **function call graph** of Windows PE malware, injecting executable dummy functions at call sites via **binary patching** with classifier-guided **simulated-annealing** search; reached **85–100% attack success** across three detectors (MalConv, MalGraph, SAFE+GNN), beating prior SOTA by up to **95pp** while preserving malicious behavior in **86–97%** of variants.
- LLM Code Security**: Training-free method contrasting an **auditor LLM's** security- vs. style-review **token probabilities** to select insecure LLM-generated code and localize likely-vulnerable lines and ranking insecure implementation, outperforming a frontier LLM judge at selection.

EDUCATION

Purdue University (Advisor: Dr. Elisa Bertino)

Indiana, USA

PhD in Computer Science (CGPA: 3.90/4.00) | MS in Computer Science (CGPA: 3.84/4.00)

Aug 2023 – Present

SELECTED PUBLICATIONS

- Md Ajwad Akil, Adrian Shuai Li, Imtiaz Karim, Arun Iyengar, Ashish Kundu, Elisa Bertino - **PhantomCall: Evading ML Malware Detectors via Function Call Graph Perturbation** - *Under Submission*
- Adrian Shuai Li, Md Ajwad Akil, Elisa Bertino - **Can Drift-Adaptive Malware Detectors Be Made Robust? Attacks and Defenses Under White-Box and Black-Box Threats** - *Preprint*
- Md Ajwad Akil, Adrian Shuai Li, Imtiaz Karim, Arun Iyengar, Ashish Kundu, Vinny Parla, Elisa Bertino - **LLMalMorph: On The Feasibility of Generating Variant Malware using Large-Language-Models** - *IEEE-TPS 2025 (Best Paper Award)*
- Gourab Saha, Shashata Sawmya, Arpita Saha, Md Ajwad Akil, Sadia Tasnim, Md Saifur Rahman, M Sohel Rahman - **PRIEST: predicting viral mutations with immune escape capability of SARS-CoV-2 using temporal evolutionary information** - *Briefings in Bioinformatics*
- Md Ajwad Akil, Najrin Sultana, Abhik Bhattacharjee, Rifat Shahriyar - **BanglaParaphrase: A High-Quality Bangla Paraphrase Dataset** - *IJCNLP-AACL 2022*

TECHNICAL SKILLS

Languages: Python, C++, Java, JavaScript

ML/LLM: PyTorch, Hugging Face, TRL, vLLM, SGLang, LangChain, LangGraph, smolagents, scikit-learn

Infra/Data: AWS, SageMaker, Modal, Docker, Git, PostgreSQL, MongoDB, Elasticsearch, ChromaDB

Security: IDA Pro, Binary Ninja, LIEF, pefile, CodeQL, FlowDroid, MobSF