Kian Esmaeili
Cybersecurity | AI/ML Security Researcher | First-Author IEEE Publication
Eskian29@gmail.com • • LinkedIn • GitHub • kianesmaeili.com • research.kianesmaeili.com

EDUCATION

Georgia Institute of Technology Atlanta, GA
Master of Science in Cybersecurity (Information Technologies)
- Expected graduation: May 2028 (Starting August 2026)

University of North Georgia Dahlonega, GA
Bachelor of Science, Cybersecurity, Minor Entrepreneurship May 2026 | Major GPA: 3.82/4.00
- Honors Thesis: AI-driven endpoint security using behavioral analysis of Sysmon telemetry
- First-author IEEE publication (SoutheastCon 2026, IEEE Xplore)
- 2x recognized in NSA/DHS Codebreaker Challenge

PUBLICATIONS

AI-Driven Update Validation in Endpoint Security - IEEE SoutheastCon 2026 (First Author, published in IEEE Xplore)

Operation North Guard: A Multi-Variant Dynamic Flag Framework for Cybersecurity Education - ISCAP 2026 (First Author, Under Review)

Misleading Performance in Sysmon-Based Machine Learning: The Impact of Data Representation and Temporal Structure - EAI Endorsed Transactions (First Author, Under Review)

RESEARCH EXPERIENCE

University of North Georgia Dahlonega, GA | Jan 2026 – Jun 2026
AI/ML Research Assistant
- Built an ML-based ransomware detection pipeline using Sysmon endpoint telemetry, collecting and labeling 6,200+ events from live ransomware executions in isolated VM environments
- Benchmarked five models (Random Forest, XGBoost, SVM, Logistic Regression, Isolation Forest), showing event-level representations inflate accuracy to near-100% while behavioral aggregation reveals true performance of 75–82%
- Identified and named "temporal collapse" and event-level feature leakage as structural biases in Sysmon-based ML evaluation - findings under review at EAI Endorsed Transactions
- Analyzed the 2024 CrowdStrike Falcon outage and AI-driven update validation frameworks; published as first-author IEEE SoutheastCon 2026 paper

Georgia Tech Research Institute Atlanta, GA | Aug 2025 – Dec 2025
Undergraduate Researcher – Embedded Systems Security (VIP Program)
- Competed in the CSAW 2025 Embedded Security Challenge, performing side-channel and fault-injection attacks on embedded targets using the ChipWhisperer-Nano platform
- Researched timing, power, electromagnetic, and acoustic side-channel methods against password-verification firmware; analyzed how early-exit and busy-wait logic produced exploitable leakage
- Investigated AI/LLM integration into side-channel workflows for automated trace alignment, classification, and key recovery
- Co-authored the team's technical paper, writing the methodology and deep-learning sections and verifying technical accuracy against IEEE/Springer sources

PROFESSIONAL EXPERIENCE

Federal Reserve Bank of Atlanta Atlanta, GA | May 2025 – Nov 2025
Supervision and Regulation (Cybersecurity, Operational Resilience and Emerging Tech)
- Defined and piloted enterprise AI use cases for cybersecurity and operational workflows within Supervision & Regulation
- Built automation tools in Microsoft Power Apps to streamline internal data analysis and reporting for examination teams
- Supported cybersecurity examinations, including critical-vendor operational resilience assessments of regulated institutions
- Placed 3rd out of ~38 teams across the Federal Reserve System in the Board AI Tournament, developing an enterprise AI orchestration concept
- Built a Power Apps platform to centralize and categorize shared resources (internal Ideathon)
- Researched FinTech firms and their partnership activity, presenting findings to the Supervision & Regulation group to inform emerging-tech risk awareness

Southern Real Estate Developers (Contract) Alpharetta, GA | Jan 2025 – Mar 2025
Web Developer/ Consultant

- Contracted through my own web-development business to design and build the company's website end to end
- Optimized the site for SEO and redesigned the interface for improved usability
- Advised on cybersecurity for both the website and internal office systems

SELECTED PROJECTS

AI-Powered Security Assistant (n8n + LLM + RAG)
Personal project

- Developed an AI-powered personal assistant using n8n, integrating ChatGPT, a vector database (RAG architecture), and Telegram for real-time interaction
- Designed automated workflows for data ingestion, semantic search, and contextual response generation
- Implemented an end-to-end pipeline combining LLMs with vector search for personalized knowledge retrieval

Cybersecurity CTF Platform – "Operation North Guard"
Capstone Project | https://ctf-six-tau.vercel.app/

- Built a full-stack Capture the Flag platform (Next.js, React, TypeScript) for hands-on cybersecurity training
- Engineered a multi-variant dynamic flag system using salted SHA-256 hashing to prevent flag-sharing and plagiarism in academic settings
- Developed 10+ challenges across network forensics, cryptography, reverse engineering, SQL injection, and cloud security, using a modular MDX-based challenge engine
- Basis for first-author ISCAP 2026 paper (under review)

TECHNICAL SKILLS

Programming: Python, SQL, PowerShell, Bash, JavaScript
Systems: Windows, Linux, Kali Linux, macOS, Unix
Cybersecurity: Sysmon, Endpoint Telemetry, Malware Analysis, Network Security, Forensics, Reverse Engineering
AI/ML: Machine Learning (classification, feature engineering, model evaluation), Behavioral Modeling
Tools: Wireshark, Nmap, Power Apps, Power BI, Git, FTK Imager
Reverse Engineering: Ghidra, IDA Pro, x64dbg, Binary Ninja, OllyDbg

Additional Experience: Retail & customer service, 2018–2026 - worked continuously since high school, throughout undergraduate and graduate studies alongside research and internships.

LEADERSHIP & HONORS

- **2x Winner, UNG Pitch Challenge -** pitched a cybersecurity venture integrating hardware, software, and network security
- **National Cyber Scholarship (SANS / CyberStart America) -** national high scorer, awarded SANS scholarship
- **University Innovation Fellow** - Stanford d.school program; presented at international UIF conference (U. of Twente, Netherlands)
- **UNG Representative, Virginia Tech & VMI Cyber Immersion Camp** - selected for hands-on training in AI/ML, networking, and cyber operations