Muhammad Rabiu

Open to travel | mrabi002@odu.edu | Cybersecurity | AI Automation & Cybersecurity Professional | SOC 2, NIST, AWS | AI Ethics| linkedin | Github

PROFESSIONAL SUMMARY

Graduate researcher and teaching assistant specializing in AI-driven cybersecurity, secure code generation, and network/database security. Experienced in bridging technical execution (secure code, LLM vulnerability research, database and systems security) with governance frameworks (SOC 2, NIST, AI ethics). Skilled at explaining complex concepts in both classroom and research settings, with a mission to align advanced AI security research with national security and compliance priorities.

EDUCATION

Old Dominion University
Norfolk, VA
Bachelor of Science in Cybersecurity, Minor: Computer Science | GPA: 3.44 | Grad. May 2025
Old Dominion University
Norfolk, VA
Master of Science in Computer Science (In Progress, Expected 2027)
Graduate Teaching Assistantship: Awarded full tuition waiver + stipend to support teaching in secure databases and network systems security.

Graduate Researcher (PromSec, under Dr. Nazzal):

- Conducting research on secure code generation with LLMs.
- Analyzing PromSec (CCS '24): algorithm using gGANs + LLMs for prompt optimization.
- Investigating new approaches for CWE vulnerability detection prior to graph conversion.
- Exploring dual-objective optimization (security + functionality) and transferability across LLMs and languages.
- Building toward next-generation AI-assisted vulnerability scanners.
- Research focus under Assistant Professor Mahmoud Nazzal on AI-driven cybersecurity and secure code generation with LLMs, working directly with the PromSec framework.
- Conducting literature review and analysis of PromSec: Prompt Optimization for Secure Generation of Functional Source Code with LLMs (CCS 2024), which integrates generative adversarial graph neural networks (gGANs) with LLM prompt optimization to mitigate vulnerabilities in AI-generated code .
- Exploring dual-objective optimization, balancing security and functionality, and investigating the transferability of optimized prompts across LLMs, CWEs, and programming languages .
- Contributing to ongoing research efforts toward trustworthy AI deployment in cybersecurity-critical contexts, bridging GRC frameworks with cutting-edge AI security methods.

Graduate Teaching Assistant, Old Dominion University

- CS 450/550: Database Concepts → assisted in assignments, grading, and guiding students in relational models, SQL security, and data integrity.
- CS 464/564: Networked Systems Security → supported labs and lectures on secure network design, cryptographic protocols, and system hardening.
- Provided one-on-one student support, helping translate complex security concepts into practical exercises.
- Certificates: CompTIA Security+, AWS Cloud Compliance (In Progress).
- Relevant Coursework: Cloud Security, AI Ethics & Governance, Cybersecurity Risk Management, Software Design, Cybersecurity Risk Assessment, Data Ethics.
- Awards/Honors: Perry Honors College, Monarch Pride Grant Recipient.

PROJECTS & TECHNICAL SKILLS

Cloud Compliance Checklist (AWS SOC 2)

Norfolk, VA
Developer/Analyst
January 2023 - April 2023

- Simulated third-party audit environment with stakeholder communication in mind.
- Demonstrated audit lifecycle awareness from risk discovery to evidence presentation.
- Conducted a SOC 2 audit simulation across AWS services (IAM, S3, CloudTrail, GuardDuty), identifying gaps and recommending control improvements.
- Created an Excel-based risk register and visual control map with evidence screenshots to support audit readiness.
- Mapped technical configurations to SOC 2 Trust Services Criteria and internal GRC templates to simulate real audits.

NIST Risk Register + Control Mapping (GRC Simulation)
Norfolk, VA
Developer/Analyst
April 2023 - May 2023

- Built a simulated GRC risk register aligned to NIST CSF for a fictional health-tech cloud provider.
- Assessed risks across AWS S3, IAM policies, and third-party APIs; prioritized mitigations and drafted internal controls.
- Delivered PDF and Excel-based documentation, including mapped NIST categories and executive-level summary.

Governance, Risk, and Compliance (GRC):
Risk Assessment, Risk Register Creation, Policy Mapping, SOC 2 Alignment, NIST CSF Framework, Audit Readiness.
Cloud Infrastructure & Compliance Tools:
AWS Services (S3, EC2, IAM, CloudTrail), Cloud Security, IAM Policies, Encryption Standards, Security Groups, Compliance Monitoring, Regulatory Documentation, Internal Control Mapping, Incident Response Process Support.
Programming & Technical Skills:
Python (Automation, GUI – Tkinter), Git/GitHub, Bash/Shell, JSON/YAML (for policy configuration), Generative Models, Cortex XDR / AI Detection Tools.Security Event Monitoring, Threat Detection & Response, Incident Triage
Data & Productivity Tools:
Excel (PivotTables, VLOOKUP, Conditional Formatting), Microsoft Word, PowerPoint, Markdown Documentation.

WORK EXPERIENCE

Project Coral – Handshake AI (MOVE Fellowship)
Remote
Fellow
09/2025 – Present

- Selected for Project Coral, a confidential red teaming initiative with a leading AI lab.
- Designed and executed adversarial prompts to probe LLM weaknesses, policy bypasses, and reasoning failures.
- Logged and analyzed attempts in Feather annotation platform; targeted diverse attack pathways to strengthen AI guardrails.
- Collaborated with fellows and project leads via Canvas, Slack, and Hubstaff while maintaining professional and client-facing standards.
- Developed insights into model vulnerabilities, adversarial testing strategies, and ethical considerations in AI safety.

Project Checkmate – Handshake AI (MOVE Fellowship)
Remote
Fellow
09/2025 - 10/2025

- Competitively selected to join Project Checkmate, a high-impact AI safety campaign with a leading AI lab.
- Conducted prompt injection and data exfiltration tests to probe LLM vulnerabilities and bypass guardrails.

- Logged and analyzed 20+ adversarial attempts per week in Feather annotation platform, targeting diverse attack pathways.
- Collaborated with fellows and STEM specialists through Canvas and Slack, contributing to systematic evaluation and improved model resilience.

MAIS Academy / CAP Society AI & Cybersecurity Hackathon
Remote
Intern
April 2025 - Present.

- Assisted with AWS security configuration reviews, GRC documentation, and cloud compliance checklist development for an AI-themed cybersecurity hackathon.
- Wrote scripts in Python to analyze security posture and automate reporting workflows.
- Assisted in threat modeling and data evaluation tasks for AI behavior prediction in national security contexts.
- Supported the launch of a multi-event hackathon focused on AI and ethical security challenges, engaging 100+ students and professionals.
- Helped design 3+ challenge tracks exploring generative AI in cybersecurity, including synthetic threat detection and LLM policy risks.
- Collaborated with technical mentors to scope industry-relevant scenarios aligned with real-world GRC dilemmas and talent pipelines.

Nonprofit Consulting Externship (Mentored by PwC Professionals)
Remote
Extern
May 2025 - August 2025

- Selected for an 8-week strategy externship working with social justice nonprofits on stakeholder impact, communication audits, and digital positioning.
- Applied PwC frameworks to assess organizational goals, identify roadblocks, and deliver growth-oriented recommendations backed by data.
- Collaborated with nonprofit leaders on a living strategy document, focused on mission clarity and measurable outcomes.

Old Dominion University
Norfolk, VA
IT Support Technician
August 2021 - May 2025

- Resolved 100+ service tickets using ServiceNow, handling login issues, MFA enrollment, and device connectivity across a 20,000-user campus network.
- Tracked, escalated, and documented issues for audit-readiness; improved documentation workflows and user experience with SOPs and tech guides.
- Managed secure provisioning of student and staff accounts via Azure AD, enhancing onboarding security.
- Trained student workers and faculty on security-conscious IT practices and self-service troubleshooting tools.

Cyber Navigator Internship Program
Charlottesville, VA
Cyber Policy Analyst
May 2024 - August 2024.

- Conducted basic security operations (SOC) triage scenarios; physical and digital risk assessments of election infrastructure in Patrick County, VA, in partnership with UVA and VCU mentors.
- Helped raise the county's LESS Baseline Score from 44.2% to 64.5% by delivering audit-ready policy documents and training sessions, assisting in initial threat triage and documentation of remediation steps.
- Created and implemented 10+ NIST-mapped security policies, including Acceptable Use, Incident Response, and Remote Access; supported audit preparation and vendor risk evaluation.

- Facilitated in-person cybersecurity workshops for registrar staff on encrypted email, password management, and secure document redaction tools.
- Developed incident response checklist and security training guidelines for non-technical users; collaborated with cross-functional teams to simulate real-world GRC response.

ACTIVITIES & LEADERSHIP EXPERIENCE

Commonwealth Cyber Initiative (COVA CCI)
Remote
Remote Undergraduate Researcher
August 2024 - December 2024

- Interfaced AI governance with national cyber policy implications to align model oversight with emerging legislative trends.
- Conducted research on AI governance risks and regulatory frameworks, including NIST AI RMF and SOC readiness, producing policy insights for cybersecurity program strategy.
- Investigated AI policy, generative model governance, and misinformation risks to assess national cybersecurity implications.
- Developed risk assessment frameworks for AI integration into critical infrastructure resilience strategies.
- Explored evaluation techniques for LLM behavior and safety risk scenarios; examined how technical findings shape policy implementation.
- Delivered formal presentations of research insights to faculty and industry professionals at a regional cybersecurity symposium.

ODU Cybersecurity Student Association
Norfolk, VA
Member
January 2024 - Present

- Participated in cybersecurity case competitions and GRC workshops.
- Engaged in peer mentorship activities for students exploring cloud security careers.

VICEROY Undergraduate Research – AI-Driven Cybersecurity
Norfolk, VA
Undergraduate Researcher
August 2023 - December 2023

- Researched AI-driven detection and response systems to combat zero-day and polymorphic cyber threats.
- Evaluated and compared traditional vs. AI-based security tools (e.g., Cortex XDR) for operational effectiveness.
- Conducted basic SOC triage, analyzed SIEM data, and flagged anomalous events for escalation using XDR.
- Analyzed ethical concerns around algorithmic bias and data governance in AI cybersecurity adoption.
- Presented findings on AI threat modeling, detection algorithms, and long-term infrastructure resilience.
- Analyze security event data from security sensors (IDS, SIEM)
- Recognize potential, successful, and unsuccessful intrusion attempts

Old Dominion University - Perry Honors College
Norfolk, VA
Resident Assistant
August 2024 - May 2025

- Facilitated community building and crisis management in on-campus housing.
- Conducted educational programs on digital safety and responsible technology use.
- Kept a record of key audits through the university portal.
- Maintained records of student conduct and incident reports in compliance with university policy.