ANVEEKSH MAHESH RAO

Boston, MA | rao.anv@northeastern.edu | 617-840-8538 | linkedin.com/in/anveekshmrao | github.com/anveeksh | anveekshmrao.com | ORCID: 0000-0005-4791-1789

RESEARCH PROFILE

Cybersecurity researcher and practitioner focused on **human-centered security**, **usable privacy**, **phishing defense**, **AI governance**, and **embedded and medical-device security**. My work examines how security systems fail when human behavior, privacy expectations, and operational constraints are treated as secondary problems. I am especially interested in building technically rigorous security mechanisms that remain understandable, auditable, and usable in real-world environments.

RESEARCH INTERESTS

Human-Centered Security and Usable Privacy: phishing susceptibility, security warnings, social engineering, behavioral security decision-making, alert fatigue, and the Nocebo Effect in digital environments.

Privacy Engineering and AI Governance: privacy-by-design, PII/PHI protection, data governance, consent, auditability, and accountability gaps in agentic AI systems that make autonomous data-access decisions.

Systems, IoT, and Embedded Security: firmware vulnerability research, medical-device security, binary analysis, fuzzing, and security risks in resource-constrained cyber-physical systems.

EDUCATION

Northeastern University, Khoury College of Computer Sciences Boston, MA
Master of Science in Cybersecurity *GPA: 3.85 / 4.0* *Sep 2025 to Expected May 2027*

Relevant Coursework: Network Security, Cryptography, Incident Response, Vulnerability Assessment, GRC, Cyber Law, Decision Making, Critical Infrastructure Protection, Security Architecture.
In Progress: Wireless and Mobile Systems Security; Special Topics in Security and Privacy.

Srinivas University Institute of Engineering and Technology Mangalore, India
Bachelor of Technology in Cyber Security and Cyber Forensics Engineering *GPA: 8.35 / 10, First Class with Distinction* *May 2024*

RESEARCH EXPERIENCE

Research Assistant, CACTi Lab Boston, MA
Advisor: Prof. Ziming Zhao *Mentor: Sagar Mohan, PhD Researcher* *Oct 2025 to Present*

- Contribute to ongoing research on firmware vulnerability analysis and medical-device cybersecurity, applying static and dynamic analysis techniques to embedded firmware targets.
- Study attack-surface characterization and vulnerability discovery methods for IoT and resource-constrained embedded systems, including binary analysis and fuzzing workflows.
- Participate in lab seminars and research discussions; contribute literature reviews, technical exploration, and early-stage research ideas on usable security in constrained environments.

Independent Researcher Remote
Human-Centered Security, Privacy Engineering, and Applied Cybersecurity *2022 to Present*

- Conduct self-directed research on phishing susceptibility, social engineering behavior, usable security design, and the Nocebo Effect in digital environments.
- Explore privacy engineering challenges including PII/PHI segregation, consent management, data minimization, anonymization, and privacy-by-design in enterprise and cloud systems.
- Design and build applied security tools including PhishGuard, Attack Path Predictor, HoneyTrap Lab, ISO 27001 Control Mapper, and a GDPR/HIPAA Risk Register.
- Write practitioner-oriented articles on GRC, ISO 27001, risk probability, and compliance automation for

professional cybersecurity audiences.

ACADEMIC PROJECTS AND REPORTS

1. **PhishGuard: ML-Based Phishing Detection with Human-Centered Behavioral Insights**
   CY5010 Research Project, Northeastern University Spring 2026
   Deliverables: research paper, ePoster, oral presentation, and open-source code release.
   Designed and evaluated a URL-based phishing detection system using Random Forest, XGBoost, and neural-network models. Achieved high benchmark accuracy while surfacing a critical limitation: the system assigned 95.4% false-positive confidence to out-of-distribution legitimate URLs, revealing a paradigm ceiling in purely ML-driven detection. This finding anchors ongoing research interest in pairing ML detection with human-centered security interventions.
2. **Cyber-Physical Risk Assessment of the Boston Energy Network**
   Khoury College of Computer Sciences, Northeastern University Dec 2025
   Advisor: Prof. Themis Papageorge.
   Applied model-based risk assessment and network science to analyze cascading-failure risks in a 16-node critical energy infrastructure model. Built a Python/NetworkX simulation aligned with DHS NIPP and NIST SP 800-82, with proposed extensions for AI-assisted OT/ICS risk assessment.
3. **Enterprise Incident Response Playbook: Phishing, Malware, and Credential Harvesting**
   CY5010, Northeastern University Feb 2026
   Developed a NIST SP 800-61 and CISA-aligned incident response playbook covering detection, containment, eradication, recovery, and post-incident analysis. Integrated human-behavioral analysis of phishing susceptibility as part of the organizational attack surface.
4. **The Nocebo Effect in Psychology and Cyber Science**
   Independent Study 2025
   Examined how negative expectations, fear-based security messaging, and digital threat perception shape user trust and decision-making. Connects social psychology literature to usable security and privacy engineering practice.
5. **HoneyTrap Lab: Cowrie Honeypot Deployment and Threat Intelligence Analysis**
   Independent Project 2025 to 2026
   Deployed a Cowrie SSH/Telnet honeypot to capture real-world attacker behavior, brute-force patterns, credential attempts, and post-compromise commands. Produced a threat-intelligence report with geolocation analysis and defensive recommendations, published as an open-source repository.

SELECTED ARTICLES AND PUBLIC WRITING

1. **GRC: A Full In-Depth Guide.** LinkedIn Article.
2. **ISO 27001: Purpose, Value, and Organizational Use Cases.** LinkedIn Article.
3. **How to Find Risk Probability in GRC: A Practical Mathematical Guide.** LinkedIn Article.
4. **The Future of GRC and ISO in Cybersecurity.** LinkedIn Article.
5. **How to Build a Cybersecurity Portfolio: A Practitioner's Guide.** Blog, anveekshmrao.com.

SELECTED PROJECTS AND OPEN-SOURCE TOOLS

1. **PhishGuard and ThreatScan** Python, ML, HTML phishguard.anveekshmrao.com
   URL-based phishing detection and malware-analysis prototype using ML models with human-centered detection framing.
2. **Attack Path Predictor** Python, NetworkX, scikit-learn, Flask github.com/anveeksh
   Models enterprise attack paths, node compromise likelihood, and adversarial movement using graph analysis and MITRE ATT&CK.
3. **HoneyTrap Lab** Cowrie, ELK Stack, Threat Intelligence github.com/anveeksh

SSH/Telnet honeypot for capturing attacker behavior, credential patterns, command usage, and post-compromise activity.

4. **Windows Event Log Monitoring** Elastic Stack, Winlogbeat, SIEM github.com/anveeksh
   SOC lab with secure log shipping, custom detection queries, and Windows security dashboards.
5. **SubdomainHunter** Python, DNS, Certificate Transparency github.com/anveeksh
   Automated subdomain enumeration using DNS brute force and certificate transparency logs for attack-surface mapping.
6. **AI-Integrated GRC Platform** Python, ML, LangChain github.com/anveeksh
   Prototype for compliance mapping, risk scoring, and GRC workflow automation across NIST CSF, ISO 27001, and SOC 2.
7. **ISO 27001 Control Mapper** JavaScript, GPT API github.com/anveeksh
   Maps internal policies to ISO/IEC 27001:2022 Annex A controls.
8. **GDPR/HIPAA Risk Register** Python, Streamlit, SQLite github.com/anveeksh
   Web application for logging, scoring, and visualizing privacy and compliance risks.

TECHNICAL SKILLS

Security Research: Vulnerability research, binary analysis, fuzzing, exploit development, firmware analysis, memory-safety concepts, CVE research, GDB, Radare2, pwntools.

Human-Centered Security: Phishing psychology, usable security design, security awareness design, social engineering analysis, behavioral decision-making, Nocebo Effect in digital contexts.

Privacy and Governance: Privacy-by-design, PII/PHI protection, GDPR, CCPA, HIPAA, data minimization, anonymization, pseudonymization, consent management, privacy impact assessment.

GRC and Compliance: NIST CSF, NIST SP 800-53, NIST SP 800-61, NIST SP 800-82, ISO 27001:2022, CIS Controls v8, CMMC, PCI-DSS, SOX ITGC, third-party risk, audit readiness.

Security Operations: SOC operations, DFIR, SIEM, threat hunting, threat intelligence, MITRE ATT&CK, incident response, Splunk, IBM QRadar, Elastic Stack, CrowdStrike, Cybereason.

AI and ML: Python, scikit-learn, XGBoost, NetworkX, LangChain, OpenAI APIs, model evaluation, risk scoring, attack-path prediction.

Networking and Systems: TCP/IP, DNS, TLS, Wireshark, Scapy, Nmap, IDS/IPS, Linux, Bash, PowerShell.

Programming and Tools: Python, C/C++, JavaScript, SQL, Assembly (basics), REST APIs, Git/GitHub, LaTeX, Burp Suite, Nessus, Qualys, Metasploit, ServiceNow, Autopsy.

Languages: English (professional), Kannada (native), Hindi (conversational), Tulu (native).

PROFESSIONAL EXPERIENCE

Co-Founder and Governance / Policy Development Lead, Cyber Tech Associates India / Hybrid
Cybersecurity consulting, training, and compliance firm *Jan 2024 to Aug 2025*

- Led cybersecurity consulting, governance documentation, and policy-development work for client environments spanning security operations, compliance, and data protection.
- Supported SOC monitoring and SIEM tuning, improving alert quality and reducing false positives through detection-rule refinement and triage process design.
- Conducted penetration testing, vulnerability assessments, and cybercrime-support engagements involving fraud, data exposure, and digital-forensics review.
- Implemented privacy and governance controls covering PII/PHI handling, consent frameworks, access control, and GDPR/HIPAA-aligned documentation.
- Designed and delivered cybersecurity, privacy, and GRC training programs for students, professionals, and client teams.

Cybersecurity Consultant and Cybercrime Investigation Support, Confidential India
Government and semi-government engagements *Mar 2020 to Sep 2025*

- Supported VAPT, security review, DFIR, and cybercrime investigation work for public-sector and government-affiliated environments.
- Assisted with digital evidence review, forensic documentation, cyberfraud investigation, and incident-analysis reporting.
- Worked on cases involving identity theft, social engineering, financial fraud, and misuse of digital platforms.

Guest Lecturer in Cybersecurity, Alva's Institute of Engineering and Technology India
Undergraduate cybersecurity and privacy instruction *Apr 2024 to Sep 2024*

- Delivered lectures and practical sessions on cybersecurity, privacy engineering, GRC, and human-centered security for undergraduate engineering students.
- Developed hands-on labs covering penetration testing, privacy-by-design, and applied security concepts.

Cybersecurity Analyst Intern, Techproxima India / Remote
SOC operations and security assessment support *Jul 2023 to Jan 2024*

- Supported SOC operations, vulnerability review, and security assessments for international client environments.
- Investigated data-handling and privacy-related issues; recommended remediation aligned with GDPR and regional data-protection requirements.

Cybersecurity Engineer, MentorBot India / Remote
Security architecture, vulnerability assessment, and compliance support *Feb 2023 to Jan 2024*

- Conducted vulnerability assessments using Nessus, Qualys, and Metasploit; supported secure architecture design and remediation planning.
- Assisted with access-control design, data-protection documentation, and ISO 27001-aligned security controls.

Cybersecurity Trainee, Tracley GSoc India / Remote
Offensive and defensive security training *Mar 2023 to Jun 2023*

- Practiced offensive and defensive workflows using Rapid7 AppSec, Cybereason EDR, Sumo Logic SIEM, and Trend Micro XDR.
- Studied phishing behavior and social-engineering patterns as part of security awareness and detection training.

Junior Security Analyst Intern, Agamya Cyber Tech Bengaluru, India
Security assessment and incident-response support *Nov 2022 to Mar 2023*

- Conducted vulnerability scans, produced assessment reports, and assisted with incident-response activities.
- Assisted with privacy-policy documentation and data-governance reviews for client environments.

CERTIFICATIONS AND PROFESSIONAL TRAINING

- **Security:** CompTIA Security+ SY0-701 (PASSED), Google Cybersecurity Professional Certificate v2, Certified Ethical Hacker training, Cisco CCST Cybersecurity, Cisco CCNA Module 3, Cisco Networking Academy: Enterprise Networking, Security, and Automation, IT Specialist in Cybersecurity and Python.
- **Compliance and Privacy:** ISO 27001:2022-Compliant Cybersecurity, ISO 9001:2015 Quality Management System.
- **AI and Governance:** AI Governance training, Securiti.ai. Full list of 47+ certifications available on LinkedIn.

SERVICE AND COMMUNITY

- **Women in CyberSecurity** Apr 2026 to Present
  Cybersecurity community volunteer supporting programming, event coordination, and inclusion outreach.

- **Lions International 317, Treasurer** Jul 2023 to May 2024
  Managed organizational finances and supported community-service initiatives.
- **6 Kar Naval Unit, National Cadet Corps, Ex-Leading Cadet** Jul 2018 to Dec 2021
  Completed leadership, discipline, and civic-service training.
- **OWASP Boston Chapter** 2026 to Present
  Participant in regional application-security community events.
- **NU CTF Club; NU Security Club; Khoury Graduate Student Association**
  Active participant in competitive security, research community, and graduate student representation.

RESEARCH ADVISORS

- **Prof. Ziming Zhao**
  Lab Director, CACTi Lab, Khoury College of Computer Sciences, Northeastern University.
  Direct research supervisor.
- **Sagar Mohan**
  PhD Researcher and Research Mentor, Northeastern University.
  Direct research mentor.

FACULTY REFERENCES

- **Prof. Themis Papageorge**
  Professor, Khoury College of Computer Sciences, Northeastern University.
- **Prof. Elizabeth Hawthorne**
  Professor and Director of Cybersecurity, Northeastern University Arlington.
- **Prof. Jose Sierra**
  Professor and Director, MS in Cybersecurity, Northeastern University Boston.
- **Prof. K. Courtney**
  Professor, Cyber Law, Khoury College of Computer Sciences, Northeastern University.
- **Prof. Aanjhan Ranganathan**
  Wireless and Mobile Systems Security, Northeastern University.
- **Prof. Jayshree Sarathy**
  Special Topics in Security and Privacy, Northeastern University.
- **Dr. Krishna Prasad K**
  Associate Professor, Srinivas University Institute of Engineering and Technology.
- **Dr. Sudhakara A M**
  Systems Head, University Computer Centre, University of Mysore.
  sudhakara@uni-mysore.ac.in

Full contact details available upon request.