Varenya Sri Mudumba

srivarenya@tamu.edu | (979) 344-8215 | College Station, TX | LinkedIn | GitHub

EDUCATION

Texas A&M University *Aug 2025 – Present*
MS in Computer Science | GPA: 4.0/4.0 (Expected: May 2027) *College Station, TX*
- Coursework: Security Engineering, Software Security, NLP, Cybersecurity Risk, Analysis of Algorithms, IUI

National Institute of Technology, Durgapur *Dec 2020 – May 2024*
B.Tech in Computer Science and Engineering | GPA: 8.84/10.00 *Durgapur, India*
- Coursework: Computer Networks, Operating Systems, Software Engineering, DSA & OOP, Advanced DBMS

SKILLS

Security : YARA, PQC, Zero-Trust, OWASP Top 10, Malware Analysis, Reverse Engineering, PenTesting
ML & NLP : Transformers, RL, ML, PyTorch, ONNX, Scikit-learn, River, NumPy, Pandas, HPRC
Languages : Python, C/C++, Rust, JavaScript, SQL, Bash
Infra : AWS, GCP, Terraform, PostgreSQL, MongoDB, OpenSearch, Kibana, Git, Linux

RESEARCH EXPERIENCE

Texas A&M University *Feb 2025 – Present*
Graduate Researcher (Advisor: Prof. Marcus Botacin) *College Station, TX*
- Evaluating YARA rule generation across 10+ ML models and implementing targeted enhancements.
- Researching novel algorithms to reduce model training time without compromising detection accuracy.

Second Thoughts: LLM Self-Correction Evaluation (Group Research) *(In Progress)*
- Evaluating five self-correction strategies across math, code, factual QA, and commonsense benchmarks.
- Proposing confidence-gated correction optimizing the fix-to-regression ratio across task types.

Texas A&M University, GAIA Lab *Dec 2025 – Present*
Student Research Assistant (Advisor: Dr. Thanos Gentimis) *College Station, TX*
- Applied transfer learning on a 6,000-sample soil dataset, dropping classification error from 12% to 6%.
- Parallelized training across HPRC GPU clusters, slashing runtime from 12 hours to 40 minutes (~94% reduction).

NIT Durgapur *Apr 2023 – Mar 2024*
Undergraduate Researcher (Advisor: Prof. Bibhash Sen) *Durgapur, India*
- Devised PSO and GA-based test pattern generation for hardware Trojan detection, improving test sensitivity.
- Published PSO-Driven Test Pattern Generation for Hardware Trojan Detection at IEEE IATMSI 2024 (link)

PROJECTS

SMCP: Secure Model Context Protocol *Feb 2026*
- Designed a quantum-safe AI protocol using hybrid KEM (Kyber-768 + X25519) with Noise XX handshakes.
- Implemented DID-based identity and WASM sanitizer to prevent spoofing, MITM, and injection attacks.

ZTBI: Zero Trust Browser Interface *Dec 2025*
- Developed a Chrome extension using DistilBERT/ONNX for real-time Indirect Prompt Injection detection.
- Engineered Hybrid Scoring and Visibility Engine to counter zero-day semantic attacks and PII exfiltration attempts.

PROFESSIONAL EXPERIENCE

Zscaler *Feb 2024 – Aug 2025*
Software Development Engineer (prev: Associate SDE, SDE Intern) *Hyderabad, India*
- Integrated ZPA zero-trust access features into an internal framework adopted by 7+ engineering teams.
- Conducted 70+ PR reviews enforcing quality and security standards across the codebase.
- Instrumented Kibana & OpenSearch dashboards for 1,000+ metrics with alerting systems integrated into Slack.

ADDITIONAL INFORMATION

- Responsibly disclosed 7 vulnerabilities across 3 open-source projects (coordinated team effort).
- Open-source contributor with 2 merged PRs into IBM Quantum's qiskit-machine-learning repository
- Active CTF competitor across web exploitation, binary analysis, reverse engineering, and forensics.
- **Work Authorization**: Eligible to work in the U.S. under CPT, no sponsorship required.