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: Software Security, NLP, Analysis of Algorithms, Cybersecurity Risk, Intelligent User Interfaces.
- Thesis: ML-based YARA rule generation for automated malware detection (Advisor: Prof. Marcus Botacin).

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.
- Published PSO-Driven Test Pattern Generation for Hardware Trojan Detection at IEEE IATMSI 2024 [link].

TECHNICAL SKILLS

Languages : C/C++, Python, Rust, JavaScript, SQL, Bash, Groovy
Frameworks : PyTorch, React.js, Node.js, Express, Pytest, Scikit-learn, OpenTelemetry
Infra & DevOps : Terraform, Ansible, Jenkins, AWS, GCP, Docker, Git, Linux, HPRC
Data & DBs : PostgreSQL, MongoDB, OpenSearch, Kibana, NumPy, Pandas, ONNX

EXPERIENCE

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).

Zscaler *Feb 2024 - Aug 2025*
Software Development Engineer (prev: Associate SDE, SDE Intern) *Hyderabad, India*
- Deployed a Pytest system of 900+ regression tests replicating real-world ZPA network traffic, integrating into Jenkins CI/CD pipelines, boosting overall test coverage by ~26% and improving release stability.
- Optimized GCP provisioning with Terraform and Ansible, reducing environment setup from 18 hours to 3 hours.
- Migrated legacy modules to a unified framework adopted by 7+ teams, cutting maintenance by ~50%.
- Conducted 70+ PR reviews enforcing quality and security standards across the codebase.
- Automated AWS sim-box setup (EC2, S3) for on-demand environment creation, eliminating idle infrastructure costs and manual provisioning effort.
- Instrumented Kibana & OpenSearch dashboards for 1,000+ metrics with alerting systems integrated into Slack.

PROJECTS

Second Thoughts: Evaluating When LLM Self-Correction Helps vs. Hurts *(In Progress)*
- Evaluating five LLM self-correction strategies across four benchmarks on Llama-3.1-8B and Mistral-7B.
- Proposing confidence-gated correction that revises only when model confidence falls below a threshold, optimizing the fix-to-regression ratio.

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.
- Built a drop-in production proxy with QUIC/TCP transport, rate limiting, and key zeroization on session close.

ZTBI: Zero Trust Browser Interface *Dec 2025*
- Developed a Chrome extension leveraging 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.

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
- Peak CodeChef rating 1893 (4-Star). 500+ problems solved on LeetCode and Codeforces.
- Served as Representative for Dept. of CSE, coordinating with 190+ students across 4 semesters at NIT Durgapur.
- **Work Authorization:** Eligible to work in the U.S. under CPT, no sponsorship required.