Devang Dhanuka

Software Engineer (AI/ML) | *Cloud-Native Systems* | *GenAI*
Rochester, NY | +1(908)935-8654 | devangdhanuka@gmail.com | linkedin.com/in/devang1304 | devang1304.github.io

EXPERIENCE

Graduate Research Assistant - AI in cybersecurity Oct 2024 – Dec 2025
Rochester Institute of Technology *Rochester, NY*

- Designed and deployed an **ML pipeline** processing **65M+ security events** (ingestion, training, inference, explainability) for graph-based threat detection, achieving **99% accuracy** on APT identification.
- Built an **explainability framework** with low-latency (3–5s) explanations delivered via a user-facing dashboard, improving analyst trust, transparency, and decision-making by **84%**.
- Validated system usability through a **270+ analyst survey**, co-authoring **two peer-reviewed papers** on explainability in AI-driven security.

Senior Engineer - Cloud Infrastructure & Security Aug 2020 – Jun 2023
Netwoven Inc. *Kolkata, India*

- Executed enterprise cloud migrations (M365, identity, data) for **10+ global clients**, deploying **Azure** infrastructure and migrating **5,000+ users** with **99.9% uptime**.
- Implemented **Zero-Trust security** (Entra ID, MFA, Conditional Access, DLP) for **25,000+ users** across multiple clients.
- Protected **3M+ IP artifacts** for a semiconductor client (20,000+ users), enforcing data governance and DLP policies.
- Built automation and observability frameworks (PowerShell, logging, alerting, cost controls) **reducing 40% manual operations**, and achieving **20–30% cloud cost reduction**.

PROJECTS

minimal-gpt (Generative Transformer Model) | ***Python, PyTorch, CUDA, Transformer*** Jul 2025 – Jan 2026

- Built **124M-param GPT-2** from scratch matching OpenAI's architecture (**Flash Attention**, weight-tying, GELU) – verified parity via pretrained checkpoint loading.
- Engineered training pipeline with **AdamW**, cosine LR warmup, mixed-precision (fp16/bf16), and **DDP** multi-GPU scaling, achieving **1.47 val loss** on Shakespeare's works.

Threat Synthesis (Security-LLM Evaluation) | ***Python, LiteLLM, Vertex AI, Streamlit*** Sep 2025 – Dec 2025

- Built an **LLM evaluation framework** extending CTI-Bench research, testing models on **8 cybersecurity tasks** (MITRE ATT&CK, IOC extraction, CVE analysis).
- Engineered **model-agnostic inference pipeline** using **LiteLLM** and **Vertex AI**, tested on foundational models but designed to evaluate **custom/fine-tuned LLMs** (Llama, Gemma, Qwen).
- Implemented semantic scoring (F1, Jaccard) with ground-truth validation, visualized via interactive **Streamlit** dashboard.

WanderAI Travel Planner (Multi-Agent System) | ***LangChain, AWS, CI/CD, Terraform, Python*** May 2025 – Jun 2025

- Designed a **multi-agent travel system** using **LangChain**, orchestrating **multi-agent** (attraction ranking, route optimization, itinerary generation) for collaborative, context-aware planning.
- Deployed as **end-to-end serverless app** on **AWS** (Lambda, DynamoDB, CloudFront) with automated CI/CD, generating personalized itineraries with $<$**3s response time**.

Financial Management Hub (Serverless AWS App) | ***AWS, Terraform, Docker, CI/CD*** Feb 2025 – Apr 2025

- Architected a **serverless** financial platform on **AWS** (Lambda, DynamoDB, Amplify) with **OpenAI** for expense categorization and **Plaid** for bank integration.
- Engineered **IaC** pipelines using **Terraform** and **Docker**, enabling auto-scaling and **CI/CD** via **GitHub Actions**.
- Achieved **99.99% uptime** with real-time transaction categorization and budget tracking.

EDUCATION

Master of Science in Data Science | Rochester Institute of Technology, Rochester, NY Aug 2023 – Dec 2025
Bachelor of Computer Applications | Amity University, Noida, India Jul 2017 – Jun 2020

PUBLICATIONS

- **"PROVEX: Enhancing SOC Analyst Trust with Explainable Provenance-Based IDS."** Dec 2025
  Devang Dhanuka, Nidhi Rastogi - XAI framework for temporal graph-based IDS with post-hoc explanations.
- **"Too Much to Trust? Measuring the Security and Cognitive Impacts of Explainability in AI-Driven SOCs."** Jul 2025
  Nidhi Rastogi, Devang Dhanuka, *et al.* - Evaluates explainability methods' effect on analyst trust and efficiency.
- **"Impact of LLMs on Team Collaboration in Software Development."** Devang Dhanuka. Aug 2024

TECHNICAL SKILLS

Languages & Core: Python, Java, SQL, Linux, PowerShell, React, Node.js
Software Engineering & ML: PyTorch, Scikit-learn, Hugging Face, REST APIs, FastAPI, Streamlit
Cloud & Architecture: AWS (Certified), Azure, GCP (Vertex AI), Kubernetes, Docker, Terraform, CI/CD
GenAI & LLM Systems: RAG, LangChain, LlamaIndex, LiteLLM, vLLM, Model Evaluation