Devang Dhanuka

ML Engineering | *GenAI* | *Cloud Infrastructure*
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*

- Co-authored **two research papers** on AI explainability for cybersecurity, collecting **270+ analyst responses** to inform the design of a deployed SOC dashboard.
- Built an end-to-end **ML pipeline** processing **65M+ security events** from DARPA datasets to train a graph-based threat detection model, achieving **99% accuracy** on APT attack identification.
- Developed an **explainability framework** for Temporal GNN-based intrusion detection, benchmarking 3 methods including a **novel explainer**. Deployed dashboard with **3-5 second explanations** that improved analyst confidence by **84%**.

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

- Architected **Infrastructure-as-Code (IaC)** pipelines and scalable **Azure** compute platforms using **Kubernetes** and **Terraform**, creating the high-performance foundation necessary for data-intensive and distributed systems.
- Enforced **Data Governance** and **DLP** (Data Loss Prevention) for **3M+ IP artifacts**, implementing **Zero-Trust** security models that align with modern **Responsible AI** and enterprise data safety standards.
- Engineered **Event-Driven Automation** and **Observability** frameworks (Logging, Alerting, Cost Optimization), reducing operational overhead by **˜40%** and ensuring financial efficiency for cloud-scale workloads.

PROJECTS

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

- Built a decoder-only **Transformer** from scratch in **PyTorch**, implementing **Multi-Head Self-Attention**, **LayerNorm**, and **Residual Connections** to reproduce the **GPT-2** architecture.
- Implemented the full pre-training loop on large-scale text data, optimizing **Cross-Entropy Loss** with **AdamW** and gaining deep intuition into **LLM** training dynamics and **Next-Token Prediction**.

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

- Built an **Automated LLM Evaluation Framework** benchmarking SOTA foundational models on 8 distinct cybersecurity tasks (e.g., **MITRE ATT&CK** mapping, **IOC** extraction), quantifying performance against ground truth.
- Architected a parallel **Multi-Agent Inference Pipeline** using **LiteLLM** and **Vertex AI**, implementing **Ensemble Voting** and semantic scoring metrics (F1, Jaccard) visualized via a custom **Streamlit** dashboard.

Travel Itinerary Planner with Google ADK Agents | ***Google ADK, Vertex AI, BigQuery*** May 2025 – Jun 2025

- Built a **multi-agent travel planning system** using **Google ADK** and **Vertex AI**; specialized agents collaborated to rank attractions and generate optimized day-by-day itineraries from user preferences.
- Deployed **serverless pipeline** with **event-driven orchestration** on **BigQuery**, enabling cost-efficient, scalable inference for real-time trip planning.

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

- Architected a **Serverless** financial intelligence platform on **AWS** (Lambda, DynamoDB, Amplify), utilizing **OpenAI** and **Plaid** APIs to deliver real-time, AI-driven expense categorization with **99.99% Uptime**.
- Engineered production-grade **Infrastructure-as-Code (IaC)** pipelines using **Terraform** and **Docker**, enabling **Auto-Scaling** and automated **CI/CD** deployments via **GitHub Actions**.

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

ML & Deep Learning: PyTorch, TensorFlow, Hugging Face, Scikit-learn, CUDA
GenAI & LLMs: LangChain, LlamaIndex, LiteLLM, vLLM, RAG, OpenAI API
Cloud & MLOps: AWS (Cloud Practitioner Certified), Azure, Vertex AI, Docker, Kubernetes, Terraform, GitHub Actions
Data & Programming: Python, SQL, PostgreSQL, BigQuery, Pandas, Streamlit, FastAPI, PowerShell, Git, Linux