

Daniel David

Software Engineer | Specialized in Scalable & Secure ML/AI Pipelines | Columbia University
New York, NY 10025 | (202) 594 4804 | daniel195700@gmail.com | linkedin/in/ddavid37 | github.com/ddavid37

WORK EXPERIENCE

Software Engineer - Rhino Federated Computing - [Link](#)

Dec 24' – Expected May 26'

- **Distributed Systems:** Engineered distributed, production-grade ML/AI pipelines using NVIDIA NVFlare while refactoring Client APIs to reduce communication latency and optimize computing efficiency for the different models. [Link](#).
- **System Reliability & Monitoring:** Implemented expanded network topology support and real-time system monitoring using Grafana, allowing for the diagnosis of latency bottlenecks in distributed learning sessions.
- **Infrastructure Optimization:** Migrated legacy federated learning examples to modern architectures by optimizing Dockerfiles and configurations, streamlining the deployment across heterogeneous compute environments.
- **Encryption & Data Integrity Mechanisms:** Architected secure model transmission protocols leveraging AWS Secrets Manager, ensuring data integrity during multi-node parameter aggregation cycles. [Link](#).
- **Documentation & Onboarding:** Authored technical documentation regarding SDK usage and platform guides, significantly reducing onboarding friction, in addition, provided technical support throughout the process. [Link](#), [Link](#).

Course Assistant - Columbia - COMS4995 Machine Learning Security [Link](#).

Jan 26' – May 26'

- Acted as course assistant to a Master-level ML&LLMs Security class along with Dr. Suman Jana.

TECHNICAL KNOWLEDGE

- **Machine Learning & AI:** Experience with RAG pipelines and agentic workflows using frameworks like LangChain and internet retrieval tools like Tavily. Core expertise in ML/DL with PyTorch, TensorFlow, scikit-learn, NumPy, Pandas. Built and deployed models for pneumonia detection and financial fraud detection at Rhino.
- **Federated Learning & Security:** Core professional expertise from Rhino Federated Computing based on NVIDIA's NVFLARE framework. Authored onboarding tutorials and developed AES+RSA encryption workflows (integrated with AWS Secrets Manager and manual key handling) aligned with enterprise and research-grade standards. [Link](#).
- **Cloud & DevOps:** Extensive professional experience with containerization (Docker) and orchestration (Kubernetes), deploying federated workloads across AWS, GCP, and Azure.
- **Databases & Data Engineering:** Proficient in SQL and PostgreSQL, with deep experience at Rhino configuring schemas, validating federated datasets, and supporting production data pipelines across healthcare and finance clients. Worked extensively with cloud database integration (AWS/GCP/Azure) to enable scalable federated workflows. Skilled in query design and schema optimization, with additional academic exposure to NoSQL systems (MongoDB, Neo4j).
- **Malware Analysis:** Completed 2 graduate courses focused on hands-on labs in reverse engineering and malware analysis using IDA Pro, OllyDbg, Procmon, FakeNet, and Wireshark. Proficient in static/dynamic analysis, anti-reversing techniques, risk and vulnerability assessment, and network security fundamentals, including DDoS attacks, man-in-the-middle attacks, password exploitation, IoT vulnerabilities, and supply chain security risks.
- **Web & App Development:** Proficient in JavaScript, CSS, React, and Bootstrap for web apps. Built interactive ML learning platforms using Flask + JS + Bootstrap with interactive quizzes, progress tracking, and responsive UI. [Link](#).
- **Programming:** Strong professional experience with Python and notebook environments at Rhino for ML pipelines and federated learning demos. Additional proficiency in Java, C, C++ and Assembly.
- **Systems & Infrastructure:** Experienced with distributed computing across multi-cloud environments, CI/CD pipelines, virtualization. At Rhino, consistently used Grafana for cloud monitoring and real-time visibility for client services.

EDUCATION

Bachelor of Science - Computer Science

Sep 22' – Expected May 26'

Overall GPA: 3.52/4.00, ML/AI track, Recipient of the "Renaissance" Honors Scholarship, Dean's List, PTK Honor Society.

SELECTED PROJECTS

Tutorial #1 – Basic Usage of Rhino FCP for Federated Learning [Link](#)

Created the flagship tutorial for the Rhino FCP to guide users through core fundamental steps of the platform's GUI.

Tutorial #2 – Tutorial #2: Using the Rhino Health Python SDK [Link](#)

Authored and maintained an advanced technical tutorial for the Rhino FCP's Python SDK. [Link](#)

Model & Code Encryption for Secure Federated Computing Workflows [Link](#)

Developed a workflow to encrypt ML models and training logic in Rhino's Federated Computing Platform, with secure key handling via AWS Secrets Manager or JSON keyfiles along with an article that now serves as an advanced reference guide.

Linear Algebraic Approaches to Neuroimaging Data Compression [Link](#)

Comparative analysis of Matrix (SVD) and Tensor (Tucker) Decomposition methods for compressing high-dimensional data.

Personal Interests: Innovation, Geography, Long-Running and Endurance Sports, Skiing, Basketball.