Datta Sai Adithya Vinjamuri

Camarillo, CA 93010
(626)737-4304 vinjamuri.dsa1@gmail.com

PROFESSIONAL SUMMARY

Analytical Computer Science graduate with hands-on experience in building and deploying machine learning applications. Skilled in Python, scikit-learn, TensorFlow, and AWS cloud tools. Demonstrated expertise in end-to-end project development, from data preprocessing to model deployment, driving impactful ML solutions in data-driven environments.

SKILLS

- Web & Mobile Development: Flask, React/Next.js, HTML/CSS, React Native, Expo, bcrypt authentication, API development
- Programming & Frameworks: Python(tensorflow, pandas, sklearn), JavaScript, SQL
- Cloud & Platforms: AWS, GCP, Microsoft Office 365.
- Data analysis: Python, PowerBI, Tableau.
- DevOps & Tools: Docker, containerization, CI/CD, Version Control.
- Scripting & Automation: APScheduler, Scripting PowerShell.

EDUCATION

California State University, Channel Islands - Camarillo, CA | Master of Science
Computer Science, 12/2025
- GPA: 3.7

Lovely Professional University - Phagwara, Punjab, India | Bachelor of Science
Computer Science And Engineering, 08/2023

EXPERIENCE

STUDENT ASSISTANT | 04/2024 - 12/2025
CSUCI - Camarillo, CA
- Developed AI transcript analyzer with chat interface using ML model trained on assist.org data, reducing manual transcript inspection by 85%.
- Supported the development a AI Chabot for our department through prompt engineering. Reduced unnecessary emails, phone calls by 35% in 4 months.
- Delivered customer service to students and staff at front desk, addressing inquiries and managing approximately 30 incoming calls and emails daily.
- Facilitated recruitment of new student assistants to enhance support for department operations.

ML INTERN | 01/2022 - 08/2023
Trillion IT services Pvt Ltd - Hyderabad, Telangana
- Built an ML model integrated into a client web application, improving user engagement by 25%.
- Developed and deployed AI-powered web features with Python, FastAPI, and React, enhancing user experience.
- Designed RESTful APIs for real-time AI predictions, facilitating seamless integration with client applications.
- Automated data workflows, increasing reporting accuracy and minimizing manual processing time.
- Assisted in cloud deployment and CI/CD pipeline setup.

PROJECTS

1) AI-Powered Penetration Testing Platform

Comprehensive full-stack cybersecurity application combining Nmap, OWASP ZAP & SQLMap orchestration with advanced AI analysis (Google Gemini 1.5 Pro). Built on a Python Flask backend in a Docker-containerized microservices architecture.

- AI Integration: Gemini-driven scan analysis, risk assessment & Q&A with caching & rate limiting
- Machine Learning: Random Forest model for automated risk scoring
- Real-time CVE Monitoring: NVD API fetcher for up-to-date vulnerability intelligence
- Reporting: Automated PDF/HTML/JSON report generation with professional styling & data visualization
- Security & Scheduling: Bcrypt auth, session management, secure API keys; APScheduler-powered cron scans with DB persistence & management UI.
- Kali Linux Integration: Embedded terminal environment for hands-on testing.
- Tech: Python, Flask, Docker, SQLite, NLTK, scikit-learn, Google Gemini API, OWASP ZAP, Nmap, SQLMap, Kali Linux, HTML/CSS/JavaScript.

2) Network Anomaly Detection System

Intelligent full-stack monitoring application that identifies real-time network anomalies using unsupervised machine learning. Built with a Python Flask backend, ML-driven detection engine, and containerized deployment architecture.

- Unsupervised ML Detection: Utilizes Isolation Forest (Scikit-Learn) to analyze multi-dimensional telemetry data (CPU usage, latency, throughput), detecting zero-day lag spikes and anomalies with 99.7% accuracy.
- High-Throughput Processing Engine: Designed with Pandas and NumPy to simulate, profile, and evaluate over 76,000 requests per second for performance stress testing and anomaly scoring.
- Secure REST API & Alerting: Developed a Flask-based REST API secured with Bcrypt authentication, integrated with an automated alerting system that simulates AWS SNS triggers when threat-confidence scores exceed 80%.
- Containerized Microservice Architecture: Deployed using Docker and Docker Compose, orchestrating the ML detection service with locally mapped volumes for isolated, zero-dependency execution.
- Tech: Python, Flask, Scikit-Learn, Pandas, NumPy, Docker, Docker Compose, Bcrypt

RELATED COURSE WORK

AWS Academy Cloud Developing (2024)

- S3, IAM, Lambda, API Gateway, DynamoDB, Elastic Beanstalk, ECS, ElastiCache, CloudFront, SNS/SQS, Kinesis, CI/CD (CloudFormation, SAM)

AWS Academy Machine Learning Foundations (2025)

- SageMaker pipelines, Autopilot, Forecast, Rekognition, Comprehend, Polly, Translate, Lex, Amazon Q Developer (gen-AI)