Bhushan Ladgaonkar

+91 9152963095 | bhushanladgaonkar@gmail.com |
LinkedIn : linkedin.com/in/bhushan-ladgaonkar | github.com/beeth73

Professional Summary

Security Researcher and Machine Learning Engineer specializing in **Adversarial AI** and **Offensive Security**. Proven experience in engineering ML-based Network Intrusion Detection Systems (NIDS) for enterprise infrastructure and researching autonomous decision-making agents using Reinforcement Learning. Seeking to leverage expertise in simulation, modeling, and security architectures.

Education

Fr. Conceicao Rodrigues College of Engineering — Mumbai, India
Bachelor of Technology (B.Tech) in Computer Engineering — *Expected May 2028*

Experience

Oil and Natural Gas Corporation (ONGC) — Mumbai, India
Summer Intern | Database & Security Group — *May 2025 – June 2025*

- Developed a prototype **Network Intrusion Detection System (NIDS)** using the UNSW-NB15 dataset to identify zero-day threats and malicious traffic patterns, addressing specific limitations in traditional signature-based detection.
- Optimized data pipelines for the **UNSW-NB15 dataset** (2M+ records) using **SMOTE** to handle class imbalance, performing advanced feature engineering to enhance model accuracy for enterprise-grade network traffic.
- Implemented and evaluated **Random Forest** and **XGBoost** algorithms, successfully reducing false positive rates while maintaining high detection sensitivity for anomalous packets.
- Collaborated with the Database Group to document threat detection methodologies, bridging the gap between raw data analysis and actionable security intelligence.

Technical Projects

TISD-Edu-AI: Local-First RAG Tutor | *Python, MLX, ChromaDB, FastAPI, LLMs* — Apr 2026

* Engineered a privacy-focused, on-device **Retrieval-Augmented Generation (RAG)** pipeline using **Microsoft Phi-3 (3.8B)** and **ChromaDB** to ground AI responses strictly in verified academic texts, eliminating educational hallucinations.
* Optimized hardware inference for Apple Silicon via the native **MLX framework**, achieving a high generation speed of **41.42 tokens/sec** and low latency (1.72s) while maintaining a minimal 9.99 GB memory footprint.
* Ingested and processed 4,600+ pages of academic PDFs into 6,400+ semantic chunks, validating system reliability with a custom evaluation suite that achieved **81.1% semantic accuracy** across a 100-sample stress test.

MendikotZero: AI Agent for Complex Trick-Taking Card Game | *Python, PyTorch, RL* — Oct 2025

* Architected a Reinforcement Learning agent capable of strategic decision-making in imperfect-information environments using the **AlphaZero architecture**.
* Implemented **Monte Carlo Tree Search (MCTS)** guided by a Dual-Head Neural Network (Policy & Value) to simulate future game states and optimize move selection.
* Designed a **Self-Play** training loop where the agent evolved strategies from random noise to advanced probability-based gameplay without human data input.

Technical Skills

Languages: Python, C, SQL, Java
AI & ML Systems: Machine Learning, Reinforcement Learning, RAG, LLMs, MCTS, PyTorch, MLX, ChromaDB, XGBoost
Security: Network Intrusion Detection (NIDS), Offensive Security, OSINT, Linux (Kali/Ubuntu), Reconnaissance
Developer Tools: Git, GitHub, FastAPI, VS Code, Jupyter Notebooks

Leadership & Involvement

Institution's Innovation Council (IIC) – FRCRCE — Mumbai, India
IPR Activities Coordinator — *Apr 2026 – Present*

* Coordinating initiatives focused on Intellectual Property Rights (IPR), patent filing, and research commercialization to foster an innovation ecosystem among engineering students.

Certifications

CS50 Cybersecurity – Harvard University
Offensive Security Operations – Cybrary
Open Source Intelligence (OSINT) – Cybrary
Cyber Kill Chain – Cybrary