LAXMI SINGH

B.Tech (ECE) Student | Cybersecurity & AI/ML Enthusiast

Kanpur, India | your-email@gmail.com | LinkedIn: linkedin.com/in/laxmi-singh-696985348 | GitHub: github.com/laxmi-singh-l

Career Objective

Motivated and detail-oriented Electronics & Communication Engineering student (B.Tech, PSIT Kanpur) passionate about Cybersecurity and Artificial Intelligence. Seeking a LinkedIn Internship to contribute to building secure AI systems, enhance threat detection models, and strengthen hands-on expertise in machine learning for cyber defense and intelligent automation.

Education

Bachelor of Technology (B.Tech) - Electronics & Communication Engineering

PSIT, Kanpur | 2024 - 2028

Technical Skills

Programming: Python, C, C++, HTML, CSS

Cybersecurity: Networking Fundamentals, Linux (Kali Linux), Wireshark, Nmap, Burp Suite, Metasploit, SOC Fundamentals, Security Monitoring

AI / Machine Learning: Machine Learning, Deep Learning, Computer Vision (OpenCV), Natural Language Processing (NLP)

Tools & Platforms: Git & GitHub, VS Code, VirtualBox, Flask, REST APIs

Projects

1. Face Recognition & Spoof Detection Security System

Tech Stack: Python, Flask REST API, PyTorch, OpenCV, CNN, MTCNN, MobileNetV2

- Built a secure face recognition system with spoof attack detection to prevent photo, video, and screen-based impersonation.
- Implemented MTCNN for face detection and FaceNet embeddings for identity recognition.
- Developed a CNN-based spoof detection model (MobileNetV2) to distinguish real vs. fake faces.
- Added liveness checks such as eye-blink detection, head-movement tracking, and frame consistency validation.
- Created a Flask-based web interface for real-time webcam processing and secure face data management.

Key Focus: AI-driven Security, Biometric Authentication, Attack Defense Mechanisms.

2. AI-Based Malware Detection System

Tech Stack: Python, scikit-learn, XGBoost, SHAP, pefile

- Designed and developed an AI-based malware detection system to classify PE files as malware or benign.
- Extracted static features (opcode frequencies, API calls) using pefile for efficient malware analysis.
- Trained and optimized ML/DL models (XGBoost, RandomForest) for binary classification.
- Integrated Explainable AI (SHAP) for model interpretability and cybersecurity transparency.

Why It Stands Out: Real cybersecurity use-case integrating ML with reverse engineering and explainability.

Strengths

- Strong problem-solving mindset
- Security-first approach in AI systems
- Hands-on experience with real-time ML models
- Fast learner and self-driven

Languages

English | Hindi

Availability

Open to LinkedIn Internships in Cybersecurity, AI, or Machine Learning

Ready for Remote / Hybrid roles