KASMYA BHATIA

kasmyakyreen@gmail.com | +91 9312316665 | Gurgaon, Haryana | github.com/kasmya | linkedin.com/in/kasmya

SUMMARY

Computer Science (AI & ML) student at Manipal University Jaipur with experience in full-stack web development, machine learning, deep learning, NLP, generative AI, and cybersecurity. Builds and deploys production-grade applications end-to-end. Published researcher in federated learning and network intrusion detection, with recognition for academic excellence and innovation.

EDUCATION

B.Tech, Computer Science & Engineering (AI & ML) 2023 – 2027
Manipal University Jaipur
Student Excellence Award (5th Semester, 2026) | **Manipal Innovation Hackathon** — Pre-Incubation Letter & Certificate of Appreciation

WORK EXPERIENCE

AI Engineer Intern | *Cybersec (Virtual)* Feb 2026 – Present
- Built ML model components and anomaly detection pipelines for a production SaaS security analytics platform; performed feature engineering, model evaluation, hyperparameter tuning, and cloud deployment of ML services.
- Engineered data preprocessing workflows for security threat detection and authored technical documentation covering model architecture, performance benchmarks, and deployment procedures.

Web Developer | *Women in CyberSecurity (WiCyS) India (Virtual)* Aug 2025 – Mar 2026
- Built and deployed a full-stack web platform using the MERN stack (MongoDB, Express, React, Node.js) with an NLP-powered chatbot, REST APIs, and Secure SDLC practices throughout the development lifecycle.
- Managed Git-based collaboration with feature branching, code reviews, and CI/CD deployment pipelines on Vercel; maintained consistent code quality across a multi-developer team.

Cybersecurity Intern | *Cisco Networking Academy, AICTE (Virtual)* Jun – Jul 2025
- Modelled enterprise network topologies and analysed traffic flow and security rule logic in Cisco Packet Tracer; applied network pattern knowledge directly to ML-based intrusion detection development.

PROJECTS & RESEARCH

FedCL-NIDS: Federated Closed-Loop Network Intrusion Detection with Automated YARA Rule Voting Consensus
Under Review — 2026 IEEE Global Symposium on Emerging and Communication Technologies | Kasmya Bhatia, Ashwarya Pradhan, Vinit Kumar Gunjan, Umashanker Sahu, Dr. Gautam Kumar — Dept. of AI & ML, Manipal University Jaipur
- Designed a federated learning architecture for distributed, privacy-preserving network intrusion detection where models train locally across decentralised nodes with no raw data sharing, ensuring scalability and data compliance.
- Built an automated YARA rule voting consensus mechanism to dynamically generate and validate threat signatures across federated nodes, reducing false positives and improving adaptability to novel attack vectors.

Personal Portfolio Website | *TypeScript · React · TanStack Router · Tailwind CSS · Cloudflare Workers*
- Designed and developed a terminal-themed personal portfolio with server-side rendering, responsive design, SEO optimisation, and edge deployment on Cloudflare Workers for fast, globally distributed load times.

API Security Analyser | *FastAPI · Scikit-learn · Isolation Forest · YARA · React · Render*
- Trained an Isolation Forest model on API request features (payload entropy, request length, traffic patterns) combined with YARA signature rules for multi-layer detection of SQLi, XSS, and zero-day threats.
- Deployed full-stack application with a live analytics dashboard, Pydantic payload validation, IP rate limiting, and persistent threat logging on Render with global CDN distribution.

WebAudit: Web Application Security Extension | *JavaScript · Chrome Extensions API · Heuristic Analysis*
- Built a Chrome/Edge browser extension performing real-time heuristic analysis of security headers, page structure, and front-end code quality; generates scored developer reports with prioritised, actionable remediation steps.

TECHNICAL SKILLS

Languages: Python, JavaScript, TypeScript, SQL, C/C++, Bash/Shell Scripting
AI / ML & Data: Deep Learning, NLP, Generative AI, LLMs, Supervised & Unsupervised Learning, Anomaly Detection, Federated Learning, Data Analysis, Feature Engineering
Libraries: Scikit-learn, TensorFlow, Keras, Hugging Face Transformers, Pandas, NumPy, Scapy, PyShark, Pydantic
Web & Backend: React, Node.js, Express, MongoDB (MERN), FastAPI, Flask, REST APIs, TanStack Router, Vite, shadcn/ui
Platforms & Tools: Git, Cloudflare Workers, AWS, Vercel, Render, Docker (familiar), MySQL
Cybersecurity: YARA Rules, API Security, Threat Modelling, Network Traffic Analysis, IDS/IPS, Secure SDLC

CERTIFICATIONS

- Google Cybersecurity Professional Certificate
- Google IT Support Professional Certificate
- Cisco Networking Academy: Python Essentials 1 & 2, Networking Essentials, Introduction to Cybersecurity, Ethical Hacker