SAURAV KUMAR

0501sauarv@gmail.com | astro-saurav.xyz | +91-9572855213 | linkedin.com/in/saurav-kumar-astro

EDUCATION

Bachelor of Computer Applications — **Apr 2023**
Manav Rachna International Institute of Research and Studies, Faridabad, India — Faridabad, *Haryana*

Kendriya Vidhalaya Kankarbagh — **Apr'22– Mar'23**
12th — Percentage: 67% — *Kankarbagh, Patna*

Kendriya Vidhalaya Manesar — **Apr'20– Mar'21**
10th — Percentage: 76% — Manesar, Haryana

RESEARCH, WORK & LEADERSHIP EXPERIENCE

Core Team Member – ML & Web Development

Spillmate (Startup) | 2025

- Contributed to conversational AI workflow design and dataset structuring for improved response quality.
- Developed and maintained web application components using React and TypeScript.
- Assisted in secure session handling and frontend-backend integration for AI-based chat systems.
- Collaborated in iterative feature deployment within startup environment.

Partner – Cybersecurity Community Operations

DCG Gurugram | Aug 2025 – Present | Hybrid

- Contribute to strategic growth and operations of a regional cybersecurity community.
- Coordinate security-focused initiatives including technical meetups and discussions.
- Collaborate with industry professionals and student communities on awareness and engagement.
- Support event planning and execution of cybersecurity and systems-security sessions.

Unreal Engine Source Contributor

Epic Games (Community Contributor) | Jan 2026 – Present | Remote

- Contribute to Unreal Engine source-level discussions and issue analysis within Epic Games developer community.
- Participate in code review conversations and community-driven problem resolution.
- Engage with engine-level architecture discussions and performance considerations

IoT Security Head

MRISA – Manav Rachna InfoSec Army | Aug 2024 – Present

- Led IoT security initiatives and mentored cybersecurity team members.
- Organized Capture the Flag (CTF) competitions and technical workshops for 100+ students.
- Designed web exploitation challenges and practical security labs.
- Promoted IoT threat awareness and defensive security best practices.

Subject Matter Expert – Cybersecurity

DG Sentinels | Aug 2024 – Present

- Delivered technical seminars and hands-on workshops on cybersecurity concepts.
- Developed structured learning content for practical security education.
- Conducted live demonstrations of attack vectors and mitigation strategies.

Awards & Competitive Achievements

- **Winner – Hacksplash 1.0**, Echelon Institute of Technology (Project: *KnoxGuard* – URL Security System) - 2023
- **8th Place – CyCog CTF 2024**, organized by IEEE MRU & MRU Cyber Squad - 2024
- **Ranked 170 / 1500+ participants – CyberHavoc CTF -** 2023
- **Winner**-INTRUSIONX, GLA University Mathura (Bad usb detector) - 2025
- **Organiser** – Cyberverse CTF -Shifting Attack Vectors - 2025
- **3rd Position** – Tech Trover (Debugging Competition) – 2023
- **Organizer** – InnoSkills Manav Rachna Lan Gaming Competition – 2024
- **Challenge Architect and CTF Developer –** CyCog CTF (0x02) at Manav Rachna University – 2025
- **Challenge Developer –** Hack or Crack CTF by DG Sentinels MRIIRS – 2025

- **Coordinator –** Enigma CTF by Manav Rachna Infosec Army – 2025
- **Finalist –** With Team Technovates at Avinya Tech Fest, IIT Guwahati - 2024

Technical Speaking & Community Leadership

- Delivered cybersecurity seminars at **Manav Rachna International Institute of Research and Studies** and **Delhi Technological University**, covering practical attack vectors and defensive strategies.
- Organized and led hands-on CTF competitions:
  - *Hack Crack* (100+ participants)
  - *Enigma CTF* (700+ participants)
- Designed and conducted **Cryptic Treasure Hunt**, a cybersecurity-themed challenge engaging 250+ students.
- Conducted Session at Delhi Technical University **(DTU)** on the topic of Emerging AI in Cybersecurity.

Technical Contributions

- Core team member for **CyCog CTF**, developed web exploitation challenges for 300+ participants.
- Core Team Member – ML & Web Development, **Spillmate (Startup)**
  ➔ Contributed to AI workflow design and web application development.

RESEARCH PUBLICATIONS

Saurav Kumar, Alan Jolly John and Sarthak Dubey **"AI-Driven Techniques for Web Search Vulnerability Identification"** February 2026

https://ieeexplore.ieee.org/document/11386307 (ieeexplore.ieee.org/document/11386307)

TECHNICAL SKILLS

Programming & Querying: Python, C, Bash, SQL (MySQL), TypeScript
Cybersecurity & Systems: OWASP Top 10, Vulnerability Assessment, Attack Surface Mapping,IoT Security, Threat Modeling, CTF Challenge Design
Frameworks & Development: PySide6, Requests, BeautifulSoup, Next.js, Firebase (Genkit), Flask
Databases: MySQL, MongoDB (Atlas)
Security Tooling & Concepts: Payload Mutation Techniques, Baseline vs Response Analysis, Severity & Confidence Classification
Systems & Environments: Linux, CLI Operations, Environment-based Configuration
Version Control: Git, GitHub

PROJECTS

KnoxGuard – Desktop URL Security Application (link)

- Developed a desktop-based malicious URL detection system to identify and block phishing and harmful links in real-time.
- Implemented URL validation logic with threat-pattern analysis and blacklist/whitelist filtering mechanisms.
- Designed a lightweight and responsive interface focused on real-time user alerts and usability.
- Structured the backend logic to support scalable rule-based threat detection.
- Tech Stack: JavaScript, React, Security Logic, Browser APIs

Ghost in the Pic – Real-Time Face Swap & Deepfake System (link)

- Built a single-image face swap application enabling real-time deepfake video processing.
- Integrated facial detection and alignment pipeline for consistent frame-level swapping.
- Optimized inference pipeline for faster processing and minimal visual distortion.
- Demonstrated practical implementation of computer vision and generative techniques.
- Tech Stack: Python, OpenCV, Deep Learning Models

Defendrix – Advanced Web Application Vulnerability Scanner (Link)
Security Research & Development Project | 2025

- Architected a modular web vulnerability scanner aligned with OWASP Top 10 standards.
- Developed automated endpoint discovery and attack surface mapping modules.
- Integrated vulnerability detection engines for SQL Injection, XSS, IDOR, and authentication flaws.
- Implemented scalable scanning workflows with structured reporting for security auditing.
- Designed reusable scanning modules following extensible architecture principles.

- Tech Stack: Python, Selenium, Flask, REST APIs, MySQL

AssistAI – AI-Powered Accessibility Companion (link)

Full-Stack AI Engineer | 2026

- Architected a multi-modal accessibility platform enabling conversational AI, real-time vision assistance, and ASL recognition using Google Gemini 2.5 Flash via Firebase Genkit.
- Designed structured AI flows using Genkit with strict Zod schema validation to enforce end-to-end type safety between LLM outputs and UI components.
- Implemented real-time camera-based object and scene understanding pipeline using image data URIs and server-side AI inference.
- Built an ASL recognition module using webcam input for hand-sign to text conversion, bridging communication gaps for hearing-impaired users.
- Developed context-aware conversational assistant with session-based memory handling and structured JSON output parsing.
- Engineered scalable server actions using Next.js 15 (App Router + React Server Components) for optimized AI request handling.
- Built fully responsive, accessible UI with keyboard navigation, ARIA labeling, focus management, and dark/light system theming.
- Configured CI-ready deployment pipeline via Firebase App Hosting with environment-based AI key management.

Tech Stack:
Next.js 15, TypeScript, Firebase Genkit, Google Gemini 2.5 Flash, Tailwind CSS, React Hook Form, Zod, Radix UI, Framer Motion, Firebase Hosting