Manoj Konda

San Jose, CA | +1 (408) 396-4802 | manoj03.work@gmail.com | kmanoj03 | kmanoj03

Education

San José State University Aug 2025 - May 2027
Master of Science in Software Engineering *San José, USA*
Coursework SW Systems Engineering, Enterprise SW Platform, SW Security Technologies

Vellore Institute of Technology Sep 2021 - May 2025
Bachelor of Technology in Information Technology CGPA: 9.00/10.00 *Vellore, IN*
Coursework Web Technologies, Cyber Security, Data Structures & Algorithms

Technical Skills

Languages: Python, Java, JavaScript/TypeScript, SQL
Web Development: React, Node.js, Express.js, NestJS, Tailwind CSS, HTML, CSS
Backend & Cloud: MongoDB, RESTful APIs, Kubernetes
Security: Threat Modeling, Input Validation, Application Security (Authorization, Secure Coding)

Work Experience

CyberMind Works Dec 2023 - Dec 2023
Full Stack Web Developer Intern (PostgreSQL, NestJS, Next.js, MikroORM, AWS, Kubernetes, Docker) *Chennai, IN*

- Engineered a scalable online code execution server for React apps using AWS EC2 and Docker, orchestrated with Kubernetes, reducing load time by approximately 30% and enabling isolated execution per user session.
- Leveraged AWS SDK to deploy dynamic, user-specific React code servers and automate data provisioning, improving server availability by 25% and cutting manual setup time by 40% enhancing overall platform reliability.
- Collaborated with the co-founder to align product goals and optimized backend code for performance by improving API response times by approximately 25% and ensuring seamless integration with the existing frontend stack.

Apple Developers Group Mar 2022 - Jul 2023
Full Stack Web Developer (HTML, CSS, React, JavaScript, MongoDB, Node.js, Python) *Vellore, IN*

- Spearheaded the development of a backend system to authenticate users, dynamically retrieve/validate Excel-based questions, streamlining the screening of 200+ applicants, reducing manual workload by 90%.
- Improved backend performance in the recruitment portal by reducing response latency by approximately 25% .
- Mitigated security vulnerabilities in the recruitment portal, strengthening authentication and data integrity.

Projects

UniRide — Typescript, Node.js, Express.js, React.js, MongoDB, Socket.io, TailwindCSS, CRON Jobs

- Architected a MERN-based ride-sharing platform for university students with modular carpool management, host-specific controls (peer reviews, host transfers, cancellations) designed to scale for 500+ concurrent ride requests.
- Integrated a real-time in-ride group chat system using Socket.io, allowing seamless communication between ride members; enhanced reliability with a CRON-based fallback system to auto-complete rides when users fail to do so manually.
- Performed threat modeling for UniRide, addressing risks in chat, authentication, and host controls, and implemented mitigations that reduced potential attack vectors by approximately 30% and improved platform reliability.

Understanding and Mitigating ARP and IP Spoofing Attacks — Ettercap, hping3, SET

- Simulated ARP and IP spoofing attacks using Ettercap and hping3, manipulating packet headers and modifying DNS records to redirect approxiamtely 80% of traffic and demonstrate real-time interception and misdirection.
- Implemented ingress/egress firewall filtering to block spoofed packets and harden the network against ARP/IP spoofing.
- Analyzed packet captures with Wireshark to trace spoofed ARP/IP traffic, verify DNS redirection behavior, and confirm the effectiveness of firewall filtering against malicious packets.

Personal Finance Tracker — MongoDB, Express.js, React.js, Node.js, Three.js, JWT, Recharts

- Built a full-stack finance tracking platform with interactive dashboards to monitor expenses, savings goals, & spending patterns in real time, visualizing 100+ sample transactions with 3D landing page (Three.js).
- Developed RESTful APIs to process real-time financial transactions with consistent sub-250ms query responses.
- Implemented input validation and JWT-based authentication to secure user financial data by successfully blocking all unauthorized login attempts in controlled test cases.