R.Srikrishna Kashyap

+918247863082 | rayabagikashyap@gmail.com | R.Srikrishna Kashyap | Kashyap Rayabagi |
LeetCode: Rayabagi Kashyap

Education

- **VIT Bhopal University** *Nov 2022 - Present*
  BTech, Computer Science and Engineering | CGPA: 8.84/10 Bhopal, India

Projects

- **WitWise: Student Collaboration App** ***Aug 2023 – Oct 2023***
  Tools: Flutter, Firebase, Dart [GitHub]
  - **Architected** cross-platform mobile application serving 500+ students with real-time document sharing, collaborative note-taking, and zero-latency synchronization using Flutter and Firebase infrastructure.
  - **Integrated** Firebase Authentication and Firestore database, achieving 30% reduction in login failures and 40% query optimization through indexed collections and advanced caching mechanisms.
  - **Implemented** role-based access control (RBAC) for students/teachers, securing 10+ subject materials with granular permissions and encrypted data transmission protocols.
  - **Enhanced** UI/UX with custom Flutter widgets and responsive design, boosting responsiveness by 35%, eliminating crashes, and reducing battery consumption by 25%.
- **Despensa: Group-based Grocery & Pantry Management Platform** ***April 2025 – May 2025***
  Tools: Spring Boot, MongoDB, MySQL, Docker, JWT, HTML/CSS/JS
  - **Developed** full-stack RESTful application with real-time CRUD operations for personal/shared grocery inventories using Spring Boot and MongoDB.
  - **Implemented** group management with role-based user assignment and shared pantry operations with access control logic.
  - **Designed** dual-database architecture: MongoDB for user/group data, MySQL for credentials with Spring Security and JWT authentication.
  - **Created** responsive frontend using HTML, CSS, JavaScript for pantry visualization and shopping list management.
- **LLM Poisoning: Security Analysis** ***Mar 2025 – Apr 2025***
  Tools: Python, HuggingFace (BERT/T5/DistilGPT), PyTorch
  - **Conducted** comprehensive security analysis simulating data poisoning attacks (factual negation, label flipping) on LLMs, demonstrating 45%+ accuracy degradation with <1% corrupted data.
  - **Analyzed** vulnerability patterns across transformer architectures (BERT, T5, DistilGPT), proving systematic overfitting to adversarial patterns and establishing baseline security metrics.
  - **Proposed** innovative defense mechanisms including statistical anomaly detection and adversarial training protocols, reducing attack effectiveness by 40% in controlled environments.
  - **Implemented** automated attack simulation frameworks using PyTorch and HuggingFace transformers, generating technical documentation and contributing to cybersecurity knowledge base.

Technical Skills

- **Programming Languages:** Python, Java, C++, Dart, SQL, JavaScript
- **Cloud & DevOps:** **AWS (Cloud Practitioner)**, CI/CD Basics, Firebase, Docker
- **Frameworks & Tools:** **Spring Boot (REST APIs, Data JPA, Maven)**, Flutter, Node.js **IBM DevOps**, **Agile Methodologies**
- **ML/AI:** PyTorch, HuggingFace Transformers
- **Databases:** MongoDB, MySQL, Firestore (NoSQL optimization)
- **Tools:** Git, IntelliJ, Postman

Certifications & Achievements

- **Certifications:** AWS Academy Cloud Foundations | AWS Academy Cloud Architecting | Coursera Networking Fundamentals | IBM DevOps Fundamentals | IBM Agile Methodologies | NPTEL Cloud Computing | NPTEL Marketing Analytics | Flipkart Grid
- **Achievements:** TCS CodeVita | Flipkart Grid Hackathon | Cyber Magazine Member
- **Languages:** English, Hindi, Kannada, Telugu