R.Srikrishna Kashyap

+91 82478 63082 | rayabagikashyap@gmail.com | R.Srikrishna Kashyap | Kashyap Rayabagi |
LeetCode: Rayabagi Kashyap

Education

- **VIT Bhopal University** *Nov 2022 - Present*
  BTech, Computer Science and Engineering | CGPA: 9.00/10 Bhopal, India

Projects

- **Despensa: Group-Based Grocery & Pantry Management Platform** ***April 2025 – May 2025***
  Tools: Spring Boot, MongoDB, MySQL, Docker, JWT, HTML/CSS/JS
  - **Developed** a backend-driven inventory management system supporting both personal and group-based pantry tracking using RESTful APIs built with Spring Boot.

    Implemented role-based group access and permissions for users to share, update, or manage grocery items collaboratively.

    Utilized MongoDB for storing pantry and group metadata, while using MySQL for credential storage secured with Spring Security and JWT tokens.

    Containerized the backend using Docker for consistent local development and simplified deployment.

    Built a lightweight web interface using vanilla HTML, CSS, and JS for managing lists and visualizing shared pantries.

- **SecureAuthX: Serverless Auth & User Management (AWS)** ***May 2025 – Jun 2025***
  Tools: AWS Cognito, API Gateway, Lambda, React, Amplify
  - **Architected** end-to-end authentication system using AWS Cognito with JWT-based access control, supporting secure sign-up, sign-in, and password reset flows across 1000+ API calls daily.

    Integrated AWS API Gateway with Lambda Authorizers for token validation and serverless backend logic, achieving sub-300ms response time and zero cold starts using optimized memory configs.

    Implemented secure React frontend with Amplify Auth and token management, reducing session-related API errors by 90% and improving user authentication flow UX.

- **LLM Poisoning: Security Analysis** ***Mar 2025 – Apr 2025***
  Tools: Python, HuggingFace (BERT/T5/DistilGPT), PyTorch
  - **Executed** comprehensive security analysis simulating data poisoning attacks (factual negation, label flipping) on 3 LLM architectures, demonstrating 45% accuracy degradation with less than 1% corrupted training data.

    Analyzed vulnerability patterns across transformer models (BERT, T5, DistilGPT) using PyTorch, identifying 15+ security flaws and establishing baseline security metrics for 50+ test scenarios.

    Created automated defense mechanisms including statistical anomaly detection and adversarial training protocols, reducing attack success rate by 40% across 100+ controlled experiments.

Technical Skills

- **Programming Languages:** Python, Java, C++, SQL, JavaScript
- **Cloud & DevOps: AWS (Cognito, Lambda, API Gateway, Amplify, IAM, CloudWatch, JWT)**, Firebase, Docker
- **Frameworks & Tools: Spring Boot (REST APIs, Data JPA, Maven)**, MongoDB, MySQL, Firestore (NoSQL optimization), Git, IntelliJ, Postman

Additional Information

- **Certifications:** AWS Academy Cloud Foundations | AWS Academy Cloud Architecting | Coursera Networking Fundamentals | Flipkart Grid
- **Achievements:** TCS CodeVita | Flipkart Grid Hackathon | Cyber Magazine Member
- **Hobbies:** Badminton, Cooking, Reading, Music
- **Languages:** English, Hindi, Kannada, Telugu