

AKSHAY O SAKHARE

+91 9766017513 | akshayosakhare@gmail.com | Pune, Maharashtra, India

LinkedIn: <https://www.linkedin.com/in/akshayosakhare> | GitHub: <https://github.com/akshayosakhare>
| Portfolio: <https://akshaysakhare.dev>

Professional Summary: Java Backend Developer with strong understanding of OOPs, Spring Boot, Hibernate/JPA, RESTful services, Microservices, and containerization. Skilled in database development using Oracle/MySQL and implement efficient and scalable backend systems. Committed to continuous learning and applying modern Java technologies in real-world projects.

Professional Development (2021 – Present):

- **Independent Research & Skill Mastery:** Committed to a comprehensive self-study program focused on modern enterprise Java development, specifically transitioning from foundational knowledge to professional-grade Spring Boot and Microservices architecture.
- **Portfolio Development:** Engineered and deployed multiple personal projects (available on GitHub/Portfolio) to demonstrate proficiency in RESTful API design, Docker containerization, and Hibernate/JPA.
- **Continuous Learning:** Actively engaged in mastering DevOps practices, including Kubernetes orchestration and CI/CD pipelines, to align with industry-standard backend engineering workflows.

Technical Skills:

- **Databases:** Oracle, MySQL.
- **Core Java:** OOPs, Collections, Multithreading, Exception Handling, Streams, Lambda Expressions
- **Frameworks:** Spring Boot, Spring MVC, Hibernate/JPA, Microservices, RESTful APIs
- **DevOps & Containerization:** Docker, Kubernetes
- **Build & Tools:** Maven, IntelliJ IDEA, Postman, Git/GitHub
- **Frontend:** HTML, CSS(Basic)

Soft Skills: Problem Solving, Technical Articulation, Cross-Functional Collaboration, Seamless Integration.

Education:

- **B.E. (Information Technology)** – Smt. Radhikatai Pandav College of Engineering, Nagpur (2021)
– 7.91 CGPA

Academic Project:

Server Intrusion Protection System: Most security solutions focus on operating systems and applications, often leaving servers vulnerable. This project fills this gap by conducting comprehensive security checks for different threat types based on predefined internal rules and permissions. Technologies used are PHP for internal logic, HTML for frontend and MySQL for hosting.