Muhammad Abdullah

+918861741751 | muhammadabdullah3602@gmail.com | www.linkedin.com/in/abd77044 | GitHub

Technical Skills

Languages: Python, Java, C/C++, SQL, HTML/CSS
Developer Tools: VS Code, PyCharm, IntelliJ, Xcode, Git, Github,
DevOps and Cloud:AWS (EC2, S3, VPC, Lambda, Cloudshell), Linux, Jenkins, Docker

Projects

CI/CD Pipeline Setup | *Jenkins, AWS EC2, GitHub, Docker* March 2025

- Set up a basic CI/CD pipeline using Jenkins to automate the build process for a Java application.
- Configured GitHub webhooks to trigger Jenkins jobs automatically on each commit, enabling continuous integration.
- Used Docker and Docker Compose to containerize the Java application and automate the build and deployment process.

Hosting a Static Web Application | *AWS, EC2, Nginx, Linux, SSH, HTML/CSS, JavaScript* February 2025

- Deployed a static web application on AWS EC2 with an Nginx web server running on Linux and established SSH access and optimized server security.
- Configured Nginx for secure and scalable hosting, enabling efficient web file serving.

Federated Learning Systems | *Python*, Machine Learning April 2024

- Inducing data poisoning attacks by maliciously generated synthetic images using a GAN
- Working on developing a server side defense strategy to mitigate the effects of the data poisoning attacks on FL systems

Stock Management System | *Python,MySQL* January 2023

- Developed a Application to scrape stock info from stock websites and store it in the database
- The stock data was scraped using the cloudscraper module in pythonand other libraries like requests, bs4 etc.
- All data will be stored in a MySQL database which is connected to python by mysql.connector

PUBLICATIONS

Label Flipping Attacks on Federated Learning: GAN-Based Poisoning and Countermeasures **2024**
Muhammad Abdullah, Vidhatri Bapu, Akash KA, Abdul Mannan Khan, M S Bhargavi

- The research paper was presented at the 2nd IEEE International Conference on Data Science and Network Security (ICDSNS) 2024, amd published by IEEE as a conference paper.
- The paper explores vulnerabilities in federated learning systems, specifically label-flipping attacks affecting global model accuracy and the security challenges faced.

Education

BANGALORE INSTITUTE OF TECHNOLOGY CGPA-8
BACHELOR OF ENGINEERING IN COMPUTER SCIENCE *2020 – 2024*

Bangalore International Academy 84%
ALL INDIA SENIOR SCHOOL CERTIFICATE EXAMINATION (CBSE) *2018 – 2020*

Christ School ICSE 85%
INDIAN CERTIFICATE OF SECONDARY EDUCATION EXAMINATION (ICSE) *2018*